第一章 集 合

§1 基本概念

集合是数学中最基本的概念，1874 年德国著名数学家 Cantor（1845－1918）发表了一篇题为《关于所有实代数数所成集合的一个性质》的论文，开创了现代集合论的研究，在 Cantor 创立集合论的时候，有一个既基本又明显的问题却一直困惑着数学家们，那就是什么是集合？对于这个问题，没有一个严格的定义。Cantor 曾给集合下过定义，大体上是说：一条性质决定一个集合，所有满足此性质的个体称为该集合的元素。在此基础上，Cantor 建立了集合论体系，即朴素的集合论体系。对于 Cantor 的集合论体系，在 1902 年 Russell 发现了悖论，即著名的 Russell 悖论。为了避免悖论和推动集合论的发展，人们逐渐地建立起公理集合论体系，本书讲述的内容属于朴素集合论，它关于集合的定义是用描述性语言给出的：

定义 当我们讨论某一类对象的时候，就把这一类对象的整体称为*集合*。

通常用大写的英文字母表示集合的名称。

定义 集合中的对象称为*元素*。

通常用小写的英文字母表示元素。

定义 设 A 为集合，a 是集合 A 中元素，则记为 $a\in A$，读做 *a 属于 A*；若 a 不是集合 A 中的元素，则记以 $a\notin A$，读做 *a 不属于 A*。

例如，所有自然数做成一个集合 A，所有多项式做成一个集合 B。

我们可以说，$3\in A$，$ax+b\in B$，$0.5\notin A$。

在集合论中，元素，集合及属于这三个概念是最基本的概念，其它概念都是由它们定义出来的。一个集合中的元素是各不相同的（无重复性），另外，集合中的元素没有先后次序（无次序性），$\{a,b\}$和$\{b,a\}$是同一集合。

集合一般有两种表示方法：

1. 列举法：列出集合中的全体元素，元素之间用逗号分开，然后用花括号括起来。

例如，设 A 是以 a,b,c,d 为元素的集合，则可表示为 $A=\{a,b,c,d\}$。

2. 描述法：用集合中元素所满足的性质表示集合。

例如，在直角坐标系中，以原点为圆心的单位圆圆周上所有点作成的集合 S 可表示如下：

$S=\{(x,y)\mid x^2+y^2=1\}$。

以上两种表示方法可以互相转化，例如，$\{x\mid x \text{是正整数}\}=\{1,2,\cdots,n,\cdots\}$。

定义 有限个元素做成的集合称为*有穷集*，无限个元素做成的集合称为*无穷集*，不含元素的集合称为*空集*，记为 ϕ。例如，$\phi\in\{\phi\}$，$\phi\notin\phi$。

定义 当 A,B 两个集合的元素完全一样时，则称集合 A,B *相等*，记为 $A=B$。

定义 设 A,B 是两个集合，若 A 的元素都是 B 的元素，则称 *B 包含 A* 或称 *A 是 B 的子集*，记为 $A\subseteq B$，若 $A\subseteq B$，且 $A\neq B$，则称 A 是 B 的*真子集*，记为 $A\subset B$。

例如，$\{1,2,3\}\subseteq\{1,2,3,4\}$，

$\{1,2,3\}\subset\{1,2,3,4\}$，

$\{1,2,3,4\}\subseteq\{1,2,3,4\}$

显然，对于任意两个集合 $A,B,A=B$ 的充要条件是 $A\subseteq B$ 且 $B\subseteq A$。这也是证明两个集合相等常用的方法。另外由定义可以看出空集是一切集合的子集且空集是唯一的。

定义 设 E 为一给定集合，如果限定所讨论的集合都是 E 的子集，则称 E 为全域集合，简称全集。这是一个相对性概念。

定义 设 A 是集合，A 的所有子集做成的集合称为 A 的幂集，记为 $\rho(A)$ 或 2^A。

例如，若 $A=\{a\}$，则 $\rho(A)=\{\phi,\{a\}\}$；$\rho(\phi)=\{\phi\}$。

显然，若 A 为有穷集，元素数为 n，则 2^A 的元素数为

$$C_n^0+C_n^1+\cdots+C_n^n=2^n$$

下面介绍集合中的几种运算：

差集：设 A,B 是两个集合，属于集合 A 而不属于集合 B 的所有元素组成的集合，称为 A 与 B 的差集，记为 $A-B$，即 $A-B=\{x\mid x\in A$ 且 $x\notin B\}$。

直乘积：设 A,B 是两个集合，所有序偶 (x,y) 做成的集合（其中 x 是 A 中的元素，y 是 B 中的元素），称为 A,B 的直乘积，记为 $A\times B$，即 $A\times B=\{(x,y)\mid x\in A$ 且 $y\in B\}$。

并集：设 A,B 是两个集合，所有属于 A 或属于 B 的元素做成的集合，称为 A 和 B 的并集，记为 $A\cup B$，即 $A\cup B=\{x\mid x\in A$ 或 $x\in B\}$。

交集：设 A,B 是两个集合，由既属于 A 又属于 B 的元素做成的集合，称为 A 和 B 的交集，记为 $A\cap B$，即 $A\cap B=\{x\mid x\in A$ 且 $x\in B\}$。

余集：设 A 是一个集合，全集 E 与 A 的差集称为 A 的余集，记为 $\sim A$，即 $\sim A=\{x\mid x\in E$ 且 $x\notin A\}$。

不难证明，对于任意集合 A,B,C 有如下算律：

1. 等幂律：$A\cap A=A, A\cup A=A$。
2. 交换律：$A\cap B=B\cap A, A\cup B=B\cup A$。
3. 结合律：$(A\cap B)\cap C=A\cap(B\cap C), (A\cup B)\cup C=A\cup(B\cup C)$。
4. 分配律：$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$，
   $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$。
5. 吸收律：$A\cap(A\cup B)=A, A\cup(A\cap B)=A$。
6. 互补律：$A\cap\sim A=\phi, A\cup\sim A=E$。
7. De Morgan 律：$\sim(A\cap B)=\sim A\cup\sim B, \sim(A\cup B)=\sim A\cap\sim B$。
8. 同一律：$E\cap A=A, \phi\cup A=A$。
9. 零一律：$\phi\cap A=\phi, E\cup A=E$。
10. 双重否定律：$\sim\sim A=A$。

例如，我们来证明：$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$。

任取 $a\in A\cap(B\cup C)$，即 $a\in A$ 且 $a\in B\cup C$，亦即 $a\in A$ 且 $a\in B$ 或 $a\in C$，于是 $a\in A\cap B$ 或者 $a\in A\cap C$，故 $a\in(A\cap B)\cup(A\cap C)$。即证得：

$$A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$$

任取 $b\in(A\cap B)\cup(A\cap C)$，即 $b\in A\cap B$ 或者 $b\in A\cap C$，亦即 $b\in A$ 且 $b\in B$，或者 $b\in A$ 且 $b\in C$。总之 $b\in A$，且 $b\in B$ 或者 $b\in C$，即 $b\in A$ 且 $b\in B\cup C$，故 $b\in A\cap(B\cup C)$。即证得：

$$(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C)$$

所以，$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$。

其余算律可类似证明。

习 题

1. 设 $S=\{2,a,\{3\},4\}$，$R=\{\{a\},1,3,4\}$指出下面的写法哪些是对的，哪些是错的：

$\{a\}\in S$，$\{a\}\in R$，$\{a,4,\{3\}\}\subseteq S$，$\{\{a\},1,3,4\}\subset R$，$R=S$，$\{a\}\subseteq S$，$\{a\}\subsetneq R$，$\phi\subseteq R$，$\phi\subseteq\{\{a\}\}\subseteq R\subsetneq E$，$\{\phi\}\subseteq S$，$\phi\in R$，$\phi\subsetneq\{\{3\},4\}$。

2. 写出下面集合的幂集合。

$\{a,\{b\}\}$，$\{1,\phi\}$，$\{X,Y,Z\}$。

3. 对任意集合 A，B，证明：

$\rho(A)\cup\rho(B)\subseteq\rho(A\cup B)$

$\rho(A)\cap\rho(B)=\rho(A\cap B)$

举例说明：$\rho(A)\cup\rho(B)\neq\rho(A\cup B)$。

§2 关 系

在日常生活中，象在数学中一样，关系的概念是一个基本概念。例如，在人群中有朋友关系，父子关系，同学关系等等；在数学中有相等关系，整除关系，小于关系，大于关系等等。不难看出，每一种关系都描述了某一集合中两个元素之间的一种特征，而这种特征也可以用一个集合描述出来。

定义 设 A，B 是两个集合，集合 $A\times B$ 的子集 R 称为 A，B 上的*二元关系*，当 $A=B$ 时，R 称为 A 上的二元关系，简称*关系*。对于 $a\in A$，$b\in B$，若 $(a,b)\in R$，则称 a，b 有关系 R，记为 aRb；若 $(a,b)\notin R$，则称 a，b 没有关系 R。

例如，自然数之间的大于关系 $=\{(x,y)\mid x,y$ 是自然数并且 $x>y\}$

人群中的父子关系 $=\{(x,y)\mid x,y$ 是人并且 x 是 y 的父亲$\}$

关系是一种特殊的集合，所以集合中的有关概念及运算在此仍然成立。

定义 设 A，B 是两个集合，R 为 A，B 上的二元关系。若 $R=\phi$，则称 R 为*空关系*；若 $R=A\times B$，则 R 称为*全关系*。

定义 设 A 为任意集合，I_A 是 A 上的二元关系，并且满足 $I_A=\{(a,a)\mid a\in A\}$，则称 I_A 为 A 上的*恒等关系*。

例如，设集合 $A=\{1,2\}$，

集合 A 上的全关系 $=\{(1,1),(1,2),(2,1),(2,2)\}$；

$I_A=\{(1,1),(2,2)\}$。

又如，设集合 $A=\{2,3,4,5\}$，集合 A 上的关系 R，S 分别为

$R=\{(a,b)\mid a,b$ 均是 A 中元素，且 a 整除 $b\}$，

$S=\{(a,b)\mid a,b$ 均是 A 中元素，且 $b=2a\}$，则

$R=\{(2,2),(3,3),(4,4),(5,5),(2,4)\}$，

$S=\{(2,4)\}$，

$R\cap S=\{(2,4)\}=S$，

$R\cup S=\{(2,2),(3,3),(4,4),(5,5),(2,4)\}=R$，

$R-S=\{(2,2),(3,3),(4,4),(5,5)\}$。

由定义容易证明：

若 R,S 是集合 A,B 上的两个二元关系，则 R,S 的交，并，差，余仍是 A,B 上的二元关系。

下面我们把二元关系推广到 n 元关系。

定义 设 $A_1,A_2,\cdots,A_n$ 为任意 n 个集合，则 $A_1\times A_2\times\cdots\times A_n$ 的任意子集 R 称为 $A_1,A_2,\cdots,A_n$ 上的一个 *n 元关系*。当 $A=A_1=A_2=\cdots=A_n$ 时，R 称为 A 上的 n 元关系。

今后我们研究的都是二元关系，并且是同一集合上的二元关系。

定义 集合 A 上的关系 R 称为有*反身性*，如果对每个 $x\in A$，都有 xRx。

例如，数的相等关系，集合的子集关系具有反身性。父子关系，数的小于关系不具有反身性。

定义 集合 A 上的关系 R 称为有*对称性*，如果 xRy，则 yRx，其中 x,y 是 A 中的元素。

例如，同学关系，三角形相似关系具有对称性。集合上子集关系，数的小于关系不具有对称性。

定义 集合 A 上的关系 R 称为有*反对称性*，如果若有 xRy，yRx，就有 $x=y$，其中 x,y 是 A 中的元素。

例如，集合上子集关系，数的小于等于关系等具有反对称性。三角形相似不具有反对称性。

定义 集合 A 上的关系 R 称为有*传递性*，如果若有 xRy，yRz，就有 xRz，其中 x,y 是 A 中的元素。

例如，数的小于关系，集合的子集关系等具有传递性。平面上直线的垂直关系不具有传递性。

由定义可以看出：

(1) 不是对称的，并非是反对称的。也就是说，对于某种关系，可能既不是对称关系，又不是反对称关系。例如，集合 $A=\{1,2,3\}$，A 上的关系 $R=\{(1,2),(1,3),(3,1)\}$，R 既不是 A 上的对称关系，又不是 A 上的反对称关系。

(2) 对于某种关系，可能既是对称的，又是反对称的。例如，当集合 $A=\{1,2,3\}$，A 上的关系 $R=\{(1,1),(2,2),(3,3)\}$，这时 R 既是 A 上的对称关系，又是 A 上的反对称关系。

当 A 是有限集合时，关系除了用集合表示外，还可以用矩阵和图形来表示，这样做不仅直观，形象，更有利于对关系的研究，也便于计算机的存储。

定义 设 $A=\{a_1,a_2,\cdots,a_n\}$，R 是 A 上的关系，称 n 阶方阵 $M_R=[r_{ij}]$ 为 R 的*关系矩阵*，其中

$$r_{ij}=\begin{cases}1, & \text{当 } a_iRa_j\\ 0, & \text{当 } a_i \text{ 与 } a_j \text{ 没有关系}\end{cases}$$

例如，设集合 $A=\{1,2,3,4\}$，R 是 A 上的一个关系，$R=\{(1,1),(1,2),(2,3),(2,4),(3,1),(3,3),(3,4),(4,2)\}$，则

$$M_R=\begin{bmatrix}1&1&0&0\\0&0&1&1\\1&0&1&1\\0&1&0&0\end{bmatrix}$$

定义 设 $A=\{a_1,a_2,\cdots,a_n\}$，R 是 A 上的一个关系，用 n 个点表示元素 $a_1,a_2,\cdots,a_n$，这些点称为结点。如果 a_iRa_j，那么由结点 a_i 到结点 a_j 作一条有向弧，箭头指向 a_j，这样的图形称为

R 的关系图。从结点 a_i 到结点 a_i 的有向弧称为自回路。

上例中的关系 R 的关系图如图 1.2.1 所示。

一般地，用关系矩阵与关系图来判断一个关系 R 是否是反身的，对称的，反对称的，传递的，有如下规律：

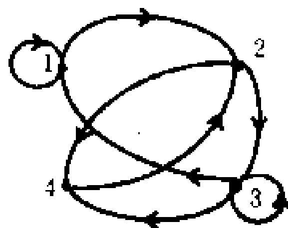


图 1.2.1

(1) 若关系 R 具有反身性，当且仅当在关系矩阵中，主对角线上元素全为 1。在关系图中每个结点都有一条自回路。

(2) 若关系 R 具有对称性，当且仅当关系矩阵是对称矩阵。在关系图中，若两个结点间存在有向弧，必是成对的。

(3) 若关系 R 具有反对称性，当且仅当关系矩阵中以主对角线对称的元素不能同时为 1，(可以同时为 0)，而主对角线上的元素可以是 1 或者 0。在关系图中两个结点间的有向弧不可能成对出现，结点可以有自回路。

(4) 若关系 R 具有传递性，关系矩阵没有明显特征。关系图的特点是：任意两个结点 a，b 间若通过一条以上的弧能连结起来的话，则必有一条从 a 到 b 的弧。

定义 设 R 是集合 A 上的一个关系，令

$$R^{-1} = \{(y,x) \mid x \in A, y \in A, \text{并且有 } xRy\}$$

则称关系 R^{-1} 为关系 R 的逆。

例如，小于关系的逆关系是大于关系，相等关系的逆关系仍是相等关系.

命题 对任意关系 R，$R=R^{-1}$ 的充要条件是 R 具有对称性。

证明：必要性，对任意 xRy，因为 $R=R^{-1}$，所以 $xR^{-1}y$，由定义有 yRx，故 R 具有对称性。

充分性，对任意 xRy，因为 R 具有对称性，所以 yRx，由定义有 $xR^{-1}y$，所以 $R \subseteq R^{-1}$。

同理，$R^{-1} \subseteq R$。故 $R=R^{-1}$。

定义 设 R，S 是集合 A 上的两个关系，令

$$R \cdot S = \{(x,y) \mid x \in A, y \in A \text{ 并且有一个 } z \in A \text{ 使得 } xRz, zSy\}$$

称为关系 R 和 S 的乘积。简记为 RS。

例如，$A=\{1,2,3,4\}$，

$R=\{(2,1),(2,3),(4,3)\}$，

$S=\{(1,2),(2,1),(2,4),(4,4)\}$

则 $RS=\{(2,2)\}$，$SR=\{(1,1),(1,3),(2,3),(4,3)\}$。由此可以看出关系乘法不满足交换律。

又如，关系的乘法满足结合律，请读者自己证明。

定理 1 集合 A 上的关系 R 具有传递性的充要条件是 $RR \subseteq R$(RR 可简记为 R^2)。

证明：必要性，任取 $(x,y) \in R^2$，于是存在 $z \in A$，使得

$$xRz, zRy$$

因为 R 有传递性，所以有 xRy。即 $(x,y) \in R$，故 $R^2 \subseteq R$。

充分性．任取 xRy，yRz，根据关系的乘积定义有 xR^2z．因为 $R^2 \subseteq R$，所以 xRz，即 R 具有传递性。

在日常生活中和在数学中，我们常常碰到对一些对象进行分类的问题。例如，对一些几何图形，我们可以使用面积之间的相等关系将这些几何图形分类，即面积相等的几何图形算做一

类，这种分类使得每个几何图形都必定属于某类，并且不同类之间没有公共元素。又如，在人群中，我们可以用同性关系将人群分类，即同性别的人算做一类。这种分类也使得每一个人都必定属于某类，并且不同类之间没有公共元素。因此，任意一个分类总是在某一观点下把一些元素看作是同样的，并且希望每一个元素在这种分类法下都必定属于而且仅仅属于某一类。具有这种功能的分类方法，在数学上就叫做一个等价关系，其严格定义如下：

定义 设 A 是一个非空集合，$\cong$是 A 上的一个关系。如果$\cong$具有反身性，对称性，传递性，则称$\cong$是一个等价关系。

例如，上面提到的几何图形的面积之间的相等关系，人群中的同性关系都是等价关系。

又如，设 $A=\{1,2,3\}$，$R=\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$，则 R 就是一个等价关系。

定义 设 A 是一个非空集合，$\cong$是 A 上的等价关系。A 的一个非空子集 M 叫做一个等价类，如果

1) 若 $a\in M$，$b\in M$，则 $a\cong b$。

2) 若 $a\in M$，$b\notin M$，则 $(a,b)\notin\cong$；或者

若 $a\in M$，$a\cong b$，则 $b\in M$。

换句话说，如果 M 中任意两个元素等价，而 M 中任意元素与 M 外任意元素不等价，则 M 就是一个等价类。

例如，上面提到的所有面积相等的几何图形就组成一个等价类(在面积相等关系下)，所有男人就组成一个等价类(在同性关系下)。

又如，设 $A=\{1,2,3\}$，$R=\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$，则存在两个等价类 $M_1=\{1,2\}$，$M_2=\{3\}$。

定理 2 设$\cong$是集合 A 上的等价关系，于是等价类是存在的。

证明：任取 $a\in A$，令

$$M=\{x\mid x\in A \text{ 并且 } x\cong a\}$$

显然，M 非空。

任取 $x_1\in M$，$x_2\in M$，由于 $x_1\cong a$，$x_2\cong a$，而$\cong$具有对称性，传递性，所以 $x_1\cong x_2$。

任取 $x_1\in M$，若 $x_1\cong y$，则由于 $x_1\cong a$，所以 $y\cong a$，故 $y\in M$。

因此，M 是一个等价类。

定理 3 设$\cong$是集合 A 上的等价关系，$M_1,M_2,\cdots$，是 A 中所有等价类。于是

$$A=M_1\cup M_2\cup\cdots$$

并且 $M_i\cap M_j=\phi(i\neq j)$。亦即，集合 A 上的等价关系把 A 分成了互不相交的等价类。

证明：任取 M_i，M_j，$i\neq j$。若有 $x\in M_i\cap M_j$，则任取 $a\in M_i$，$b\in M_j$，都有 $a\cong x$，$b\cong x$，故 $a\cong b$，所以 $M_i=M_j$，矛盾。

任取 $a\in A$，令

$$M=\{x\mid x\in A \text{ 并且 } x\cong a\}$$

由定理 1 知，M 是等价类，故有 k，使得 $M=M_k$。因为 $a\in M$，所以 $a\in M_1\cup M_2\cup\cdots\cup M_k\cup\cdots$。故 $A\subseteq M_1\cup M_2\cup\cdots$。另外显然有 $M_1\cup M_2\cup\cdots\subseteq A$。

故 $A=M_1\cup M_2\cup\cdots$。

下面我们讨论另一种重要的关系——部分序关系。

定义 设 R 是集合 A 上的一个关系。如果 R 具有反身性、反对称性、传递性，则称 R 为一个部分序关系(或称半序关系)。集合 A 在部分序关系 R 下做成一个部分序集(或半序集)，记

作(A,R)。

显然，一个部分序集的子集仍为部分序集。

例如，集合中的子集关系就是一个部分序关系，由一些集合做为元素而做成的集合，在集合的子集关系下是一个部分序集。

通常，将部分序关系 R 写做$\leq$，读做"小于或等于"。

又如，设集合 $A=\{1,2,3\}$，R 是 A 上的二元关系，$R=\{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}$，由于 R 具有反身性，反对称性，传递性，故 R 是部分序关系。

定义 一个部分序集$(A,\leq)$说是一个*序集*，如果对 A 中任意两个元素 a，b，必有 $a\leq b$ 或者 $b\leq a$。序集有时也称为链。

显然，序集的子集仍为序集。

例如，数的集合在数的大小关系下做成一个序集。

下面我们来介绍部分序集中一些特殊元素。

设$(A,\leq)$是一个部分序集，如果 A 中有一个元素 a，对于所有的 $x\in A$，都有 $x\leq a$($a\leq x$)，则称 a 为集合 A 的*最大(最小)元素*。

A 中元素 a 说是一个*极大(极小)元素*，如果除 a 之外，A 中没有元素 x，使得 $a\leq x$($x\leq a$)。

对于 A 的子集 M，A 中元素 a 称为子集 M 的一个*上界(下界)*，如果对 M 中任意元素 m，都有 $m\leq a$($a\leq m$)。M 的上界(下界)未必在 M 中，甚至 M 未必有上界(下界)。

对于 A 的子集 M，A 中元素 a 称为子集 M 的*最小上界(或称上确界)*，如果 a 是 M 的一个上界，并且对 M 的任意一个上界 x，都有 $a\leq x$。

同理，可定义 M 的*最大下界(或称下确界)*。

一个部分序集，可以用所谓 Hasse 图直观地表示出来。Hasse 图的画法如下：以平面上的点代表部分序集中的元素。

1) 由于关系$\leq$是反身的，所以在原关系图中每个结点上都有自回路，为了作图方便，省略每个结点上的自回路。

2) 由于关系$\leq$是反对称的，在原关系图中如果结点 a 与 $b(a\neq b)$之间有弧，一定是单向的，我们规定，如果 $a\leq b$，就把 b 画在 a 的上方，也就是把原关系图中结点的位置做适当调整，使得所有的弧的方向都是向上的，这样可以略去弧上的箭头。

3) 由于关系$\leq$是传递的，若 $a\leq b$，$b\leq c$，则 $a\leq c$，即从 a 到 b 有一条弧，从 b 到 c 也有一条弧，我们规定，省略掉从 a 到 c 的一条弧。也就是说，若某两结点之间有一连串带箭头的头尾相接的弧连接，那么就省略掉这两结点间的一条弧。

例如，设集合 A 上具有整除关系 $|$，试对(1)$A=\{1,2,3,4,5,6\}$，(2)$A=\{2,3,6,12,24,36\}$分别画出部分序集$(A,|)$的 Hasse 图。

解 先写出整除关系 $|$：

(1) $|=\{(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(2,2),(2,4),(2,6),(3,3),(3,6),(4,4),(5,5),(6,6)\}$

(2) $|=\{(2,2),(2,6),(2,12),(2,24),(2,36),(3,3),(3,6),(3,12),(3,24),(3,36),(6,6),(6,12),(6,24),(6,36),(12,12),(12,24),(12,36),(24,24),(36,36)\}$

(1)与(2)的 Hasse 图分别由图 1.2.2 与图 1.2.3 表示。

图 1.2.3 所代表的部分序集中无最大元素、最小元素。但是有极大、极小元素。24、36 是极

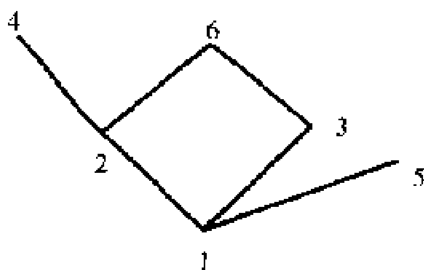


图 1.2.2

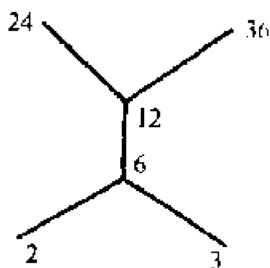


图 1.2.3

大元素，2，3 是极小元素。对于子集{2，3}，6 是其最小上界，但是，此子集无下界，当然更没有最大下界。

定义 设 R 是集合 A 上的二元关系，R 的反身(对称，传递)闭包为满足下列条件的关系 R'：

(1) R' 是反身的(对称的，传递的)；

(2) $R \subseteq R'$；

(3) 若 R'' 是反身的(对称的，传递的)，且有 $R \subseteq R''$，则必有 $R' \subseteq R''$。

R 的反身闭包记作 $r(R)$，对称闭包记作 $s(R)$，传递闭包记作 $t(R)$。

下面给出求这几种闭包的定理，关于它们的证明部分请读者自己给出。

定理 4 设 R 是集合 A 上的二元关系，I_A 是集合 A 上的恒等关系，则 $r(R)=R \cup I_A$。

定理 5 设 R 是集合 A 上的二元关系，则 $s(R)=R \cup R^{-1}$。

定理 6 设 R 是集合 A 上的二元关系，则 $t(R)=R \cup R^2 \cup R^3 \cup \cdots$。

推论 设 R 是有限集合 A 上的二元关系，A 的元数为 n，则有 $t(R)=R \cup R^2 \cup \cdots \cup R^n$。

例如，设集合 $A=\{1,2,3,4\}$，R 是集合 A 上的关系，$R=\{(1,2),(2,1),(2,3),(3,4)\}$，求 $r(R)$，$s(R)$，$t(R)$。

解 $I_A=\{(1,1),(2,2),(3,3),(4,4)\}$

$R^{-1}=\{(2,1),(1,2),(3,2),(4,3)\}$

$R^2=\{(1,1),(1,3),(2,2),(2,4)\}$

$R^3=\{(1,2),(1,4),(2,1),(2,3)\}$

$R^4=\{(1,1),(1,3),(2,2),(2,4)\}$

$r(R)=R \cup I_A=\{(1,1),(1,2),(2,1),(2,2),(2,3),(3,3),(3,4),(4,4)\}$

$s(R)=R \cup R^{-1}=\{(1,2),(2,1),(2,3),(3,2),(3,4),(4,3)\}$

$t(R)=R \cup R^2 \cup R^3 \cup R^4=\{(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4),(3,4)\}$

习　　题

1. 设 R，S 是集合 A 上的两个关系，试证明下列等式：

$(RS)^{-1}=S^{-1}R^{-1}$

$(R^{-1})^{-1}=R$

$(R \cup S)^{-1}=R^{-1} \cup S^{-1}$

$(R\cap S)^{-1}=R^{-1}\cap S^{-1}$

2. 设 R 是集合 A 上的关系。令

$$R^{+}=\{(x,y)\mid x\in A,y\in A \text{ 并且存在 } n>0,\text{使得 } xR^{n}y\}$$

证明 R^{+} 是 R 的传递闭包。

3. 若非空关系 R 是不反身的，是对称的，试证明 R 不是传递的。

4. 若集合 A 上的关系是对称的，反对称的，试指明关系 R 的结构。

5. 设 R 是非空集合 A 上的关系，如果

1）对任意 $a\in A$，都有 aRa。

2）若 aRb,aRc，则 bRc。

证明：R 是等价关系。

6. 有人说："等价关系中的反身性可以不要，因为反身性可以从对称性和传递性推出：由对称性，从 $a\cong b$ 可得 $b\cong a$，再由传递性得 $a\cong a$"。你的意见呢？

7. 若集合 A 上的关系 R、S 具有对称性，证明：RS 具有对称性的充要条件为 $RS-SR$。

8. 若 R 是等价关系，试证明 R^{-1} 也是等价关系。

§3 映 射

映射是数学上一个基本概念，也是一种特殊的二元关系。

定义 设 A 和 B 是两个任意非空集合，σ 是 A,B 上的一个二元关系，若对于每一个 $a\in A$，都有唯一的 $b\in B$，使 $(a,b)\in\sigma$，则称关系 σ 为从 A 到 B 的映射，记作 $\sigma:A\to B$。

对于 $(a,b)\in\sigma$，称 a 为原象，称 b 为 a 的象，记作 $\sigma(a)=b$。集合 A 称为映射 σ 的定义域。

设 $\sigma(A)=\{b\mid\sigma(a)=b,\text{对所有的 } a\in A\}$，称为 σ 的值域，或象的集合。

映射与一般的关系有如下的重要区别：

映射对于集合 A 中的每一个元素都有象且象唯一，而关系没有这一严格规定。

定义 设 σ 和 τ 是从集合 A 到 B 的两个映射，若对于所有的 $a\in A$，都有 $\sigma(a)=\tau(a)$，则称映射 σ 和 τ 相等，记作 $\sigma=\tau$。

下面介绍几种特殊映射。

定义 设 σ 是从集合 A 到 B 的映射，

(1) 若 $\sigma(A)=B$，则称 σ 为从 A 到 B 的满射；

(2) 若当 $a\neq b$ 时，有 $\sigma(a)\neq\sigma(b)$；或若当 $\sigma(a)=\sigma(b)$ 时必有 $a=b$，则称 σ 为从 A 到 B 的单射，或称一对一映射；

(3) 若 σ 既是满射又是单射，则称 σ 为从 A 到 B 的双射，或称一一对应映射。

例如，

(1) 设 τ 是正整数到整数的映射，$\tau(n)=$ 小于 n 的完全平方数，则

$$\tau=\{(1,0),(2,1),(3,1),(4,1),(5,2),\cdots\}$$

故 τ 既不是满射，又不是单射，更不是双射。

(2) 设 τ 是实数到实数的映射，$\tau(r)=2r-10$，则 τ 既是满射、又是单射，所以也是双射。

(3) 设 τ 是正整数到实数的映射，$\tau(n)=\lg n$，当 $m\neq n$ 时，显然有 $\lg m\neq\lg n$，故 τ 是单射。又因为 m 在正整数中取值，所以 $\lg m$ 不可能取遍实数，所以 τ 不是满射，当然也不是双射。

定义 设 $\sigma:A\to B$ 是双射，σ 的逆关系称为 σ 的逆映射，记作 $\sigma^{-1}:B\to A$。

显然，σ^{-1}也是双射，并且对任意 $a\in A$，都有 $\sigma^{-1}(\sigma(a))=a$。

定义 设 σ 是集合 A 到集合 B 内的映射，τ 是集合 B 到集合 C 内的映射，则映射 τ 与映射 σ 的乘积是一个从 A 到 C 的映射，记作 $\tau\sigma$，即

$$\tau\sigma=\{(a,c)\mid a\in A, c\in C,\text{且存在 } b, b\in B,\text{使得 } b=\sigma(a), c=\tau(b)\}.$$

不难证明：映射的乘积满足结合律，但是不满足交换律。

鸽巢原理 如果 m 个鸽子飞进 n 个鸽笼中，则至少有一个鸽笼中有 k 个或 k 个以上个鸽子，其中

$$k=\begin{cases} m/n & \text{如果 } n \text{ 整除 } m \\ [m/n]+1 & \text{否则} \end{cases}$$

例如，试证在 n 个自然数中，总能找到 k 个数$(1\leq k\leq n)$，使它们的和被 n 整除。

证明：设这 n 个自然数为 $a_1,\cdots,a_n$，考虑如下一组数：

$b_1=a_1$

$b_2=a_1+a_2$

.

.

.

$b_n=a_1+a_2+\cdots+a_n$

用 n 去除 $b_1,\cdots,b_n$，设余数分别是 $r_1,\cdots,r_n$，

(1) 若余数有一个是零，则问题已证；

(2) 若 $r_1,\cdots,r_n$ 均不为零，因在 0 与 n 之间不为 0 的数只可能是 $1,2,\cdots,n-1$ 共 $n-1$ 个，所以 $r_1,\cdots,r_n$ 必有两个余数一样，设为 $r_i,r_j,i<j$，则 n 能整除 $b_j-b_i=a_{i+1}+\cdots+a_j$。

定义 如果集合 A 是有穷集或 A 可以与自然数集合 N 建立双射，则称集合 A 是可数集合；元素个数不是有限的可数集合称为可数无穷集合；若 A 不是可数集合，则称 A 为不可数集合。

不难证明，对于可数无穷集合，可以把它的元素编号：

$$a_1,a_2,\cdots,a_n,\cdots$$

例如，所有整数集合是可数集合。

整数与自然数的一一对应关系如下：

x----1 当 $x=0$

x----$2x$ 当 $x>0$

x----$2|x|+1$ 当 $x<0$

定理 1 可数集合的子集仍为可数集合。

证明：1) 若此可数集合为有穷集，则其子集仍为有穷集，显然是可数集合；

2) 若此可数集合为无穷集，则此集合中的元素可表为

$$a_1,a_2,\cdots,a_n,\cdots \tag{1}$$

它的子集可以这样编号：从左向右看(1)，第一个是子集中元素的记为 a_{i_1}，第二个是子集中元素的记为 a_{i_2}，…，于是，此子集的元素可表为

$$a_{i_1},a_{i_2},\cdots,a_{i_n},\cdots.$$

由定义知，此子集是可数集合。

定理 2 全体实数做成的集合是不可数集合。

证明:由上一个定理知,只要证明(0,1)区间内的实数不可数就可以了。

若不然,我们可以把(0,1)区间内的数排成一个序列:

$$\left.\begin{array}{l} 0.a_{11}a_{12}a_{13}\cdots \\ 0.a_{21}a_{22}a_{23}\cdots \\ 0.a_{31}a_{32}a_{33}\cdots \end{array}\right\} \tag{2}$$

$$\vdots$$

我们考虑下面的数:

$$0.r_1r_2\cdots r_k\cdots \tag{3}$$

其中

$$r_k=\begin{cases}1 & a_{kk}\neq 1\\ 2 & a_{kk}=1\end{cases}\quad k=1,2,\cdots$$

显然,(3)是(0,1)区间内的数,但它却不是序列(2)中的任一个数。事实上,对(2)中任一个数 $0.a_{k1}a_{k2}\cdots a_{kk}\cdots$,因为 $r_k\neq a_{kk}$,故 $0.a_{k1}\cdots a_{kk}\cdots\neq 0.r_1\cdots r_k\cdots$,与假设矛盾。故(0,1)区间内的实数不可数,所以实数集不可数。

定理 3 集合 A 的元素不能与 A 的所有子集建立一一对应映射。

证明:假定 σ 为 A 到 A 的所有子集作元素的集合上的一个一一对应,令

$$B=\{x\mid x\in A \text{ 并且 } x\notin\sigma(x)\}$$

于是,存在唯一一个元素 $b\in A$,使得

$$\sigma(b)=B。$$

若 $b\in B$,则由 B 的定义知,$b\notin\sigma(b)$,即 $b\notin B$,矛盾。

若 $b\notin B$,即 $b\notin\sigma(b)$,于是由 B 的定义知,$b\in B$,矛盾。

因此,在 A 与 A 的所有子集作元素的集合之间,不能建立一一对应。

下面我们讨论集合的势与连续统问题。

定义 设 A,B 是两个集合,如果 A,B 之间存在一一对应,则称 A,B 等势,记作 $|A|=|B|$。

例如,整数集合与自然数集合等势。有理数集合与自然数集合等势。

若两个有穷集合等势,则它们的元数相等。

定义 等势关系是等价关系,它把所有集合分成等价类,等价类的名字叫做该等价类中集合的基数。

所有的可数无穷集合基数都相同,记为 ξ_0,所有与(0,1)区间等势的集合基数记为 ξ_1 或 C。

下面我们给基数规定大小:

设 A,B 是集合,若 A 与 B 的一个子集可以建立一一对应,则规定 $|A|\leq|B|$,若 $|A|\leq|B|$ 且 $|A|\neq|B|$,则规定 $|A|<|B|$。

连续统问题 按照基数的大小可排为:

$$1,2,\cdots,n,\cdots,\xi_0,\cdots,\xi_1,\cdots$$

是否存在集合 S,使得

$$\xi_0<|S|<\xi_1$$

1938 年,Godel 证明了连续统问题与集合论公理是相容的,即证明连续统问题不成立是不可能的。

1963 年,Cohem 证明了连续统问题与集合论公理是独立的,即证明连续统问题成立是不可能的。

因此,所谓连续统问题是不可能解决的。

习　题

1. 证明:映射的乘法满足结合律,举例说明:映射的乘法不满足交换律。

2. 设 σ 是集合 M 到集合 N 内的映射。证明:对 M 的任意子集 A,B,有

$$\sigma(A \cap B) \subseteq \sigma(A) \cap \sigma(B)$$

举例说明:$\sigma(A \cap B)=\sigma(A) \cap \sigma(B)$不成立。

3. 设 σ 是集合 M 到集合 N 内的映设。A 是 N 的子集,M 中所有在 σ 下映射到 A 中的元素集合称为 A 的逆象集,记为 $\sigma^{-1}(A)$。若 A,B 是 N 的任意子集,求证:$\sigma^{-1}(A \cap B)=\sigma^{-1}(A) \cap \sigma^{-1}(B)$。

4. 证明:全体整数做成的集合,全体有理数做成的集合都是可数集合。

第二章　命题逻辑

§1　基本概念

命题逻辑研究的对象是命题。所谓命题是指一句有真假意义的话。

例如,"北京是中国的首都"是命题,而且它是真的;"长春是中国最大的城市"是命题,但它是假的。

"关门!","你上哪?"这种命令和问话,不是命题。

下面,命题用大写英文字母 $P,Q,\cdots,P_1,P_2,\cdots$,表示。

如果一个命题是真的,就说它的真值是 1;如果一个命题是假的,就说它的真值是 0。我们也用 1 代表一个抽象的真命题,用 0 代表一个抽象的假命题。

定义　设 P 是一个命题,命题"P 是不对的"称为 P 的否定,记以 $\neg P$,读作非 P。$\neg P$ 是真的当且仅当 P 是假的。

例如,P:上海是一个城市。

　　$\neg P$:上海不是一个城市。

定义　设 P,Q 是两个命题,命题"P 或者 Q"称为 P,Q 的析取,记以 $P\vee Q$,读作 P 或 Q。规定 $P\vee Q$ 是真的当且仅当 P,Q 中至少有一个是真的。

例如,P:今天下雨,

　　Q:今天刮风,

　　$P\vee Q$:今天下雨或者刮风。

定义　设 P,Q 是两个命题,命题"P 并且 Q"称为 P,Q 的合取,记以 $P\wedge Q$,读作 P 且 Q。规定 $P\wedge Q$ 是真的当且仅当 P 和 Q 都是真的。

例如,P:$2\times 2=5$,

　　Q:雪是黑的,

　　$P\wedge Q$:$2\times 2=5$ 并且雪是黑的。

定义　设 P,Q 是两个命题,命题"如果 P,则 Q"称为 P 蕴涵 Q,记以 $P\rightarrow Q$。规定,$P\rightarrow Q$ 是假的当且仅当 P 是真的而 Q 是假的。

例如,P:$f(x)$是可微的,

　　Q:$f(x)$是连续的,

　　$P\rightarrow Q$:若 $f(x)$是可微的,则 $f(x)$是连续的。

显然,由定义知,当 P 是真的,Q 是真的时,命题 $P\rightarrow Q$ 是真的。这和日常生活中语言"如果…则…"的意思是一致的。但由定义知,如果 P 是假命题,则不管 Q 是什么命题,命题"如果 P,则 Q"在命题逻辑中都被认为是真命题。

例如,P:$2\times 2=5$,

　　Q:雪是黑的,

于是,命题"如果 $2\times 2=5$,则雪是黑的"是真命题。这是和人们日常生活中语言不一致的地方。

定义 设 P,Q 是两个命题,命题"P 当且仅当 Q"称为 P 等价 Q,记以 $P \leftrightarrow Q$。规定,$P \leftrightarrow Q$ 是真的当且仅当 P,Q 或者都是真的,或者都是假的。

例如,$P: a^2+b^2=a^2$,

$Q: b=0$,

$P \leftrightarrow Q: a^2+b^2=a^2$ 当且仅当 $b=0$。

下面,我们用大写的英文字母 P,Q,R,…等代表一个抽象的命题,或称为命题符号。

定义 命题符号称为原子。

例如,Q,S,…等都是原子。

定义 命题逻辑中的*公式*,是如下定义的一个符号串:

(1) 原子是公式,

(2) 若 G,H 是公式,则$(\neg G)$,$(G \vee H)$,$(G \wedge H)$,$(G \rightarrow H)$,$(G \leftrightarrow H)$是公式。

(3) 所有公式都是有限次使用(1),(2)得到的符号串。

为了省括号,有如下规定:

1. 公式$(\neg G)$的括号可以省略,写成$\neg G$。
2. 整个公式的最外层括号可以省略。
3. 五种逻辑连结词的优先级按如下次序递增:

$$\leftrightarrow, \rightarrow, \wedge, \vee, \neg$$

例如,我们写符号串

$$P \wedge Q \vee R \rightarrow Q \wedge \neg S \vee R$$

就意味着是如下公式:

$$((P \wedge (Q \vee R)) \rightarrow (Q \wedge ((\neg S) \vee R)))$$

由定义知,公式是由命题符号,逻辑连结词,括号组成的符号串,而命题符号是抽象的,所以,如果不对命题符号给以解释(即指定命题符号为真或假),则公式没有真值可言。反之,若对所有命题符号都给以解释,则公式就变成一个有真值的命题。

定义 设 G 是命题公式,$A_1, \cdots, A_n$ 是出现在 G 中的所有原子。指定 $A_1, \cdots, A_n$ 的一组真值,则这组真值称为 G 的一个*解释*。

设 G 是公式,I 是 G 的一个解释,显然,G 在 I 下有真值,通常记为 $T_I(G)$。

例如,$G=P \wedge Q$,设解释 I,I' 如下:

I:

P	Q
1	1

I':

P	Q
1	0

则 $T_I(G)=1$,$T_{I'}(G)=0$

定义 公式 G 在其所有可能的解释下所取真值的表,称为 G 的*真值表*。

显然,有 n 个不同原子的公式,共有 2^n 个解释。

例如,$G=(P \wedge Q) \rightarrow R$,其真值表如下:

P	Q	R	G
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

若公式 G 中出现的所有原子为 $A_1,\cdots,A_n$，有时我们用$\{m_1,\cdots,m_n\}$表示 G 的一个解释 I，其中

$$m_i=\begin{cases}A_i & \text{当 } A_i \text{ 在 } I \text{ 下为 1 时} \\ \neg A_i & \text{当 } A_i \text{ 在 } I \text{ 下为 0 时}\end{cases}\quad i=1,\cdots,n$$

例如，上例公式 G 的真值表中第二个解释就可以记为$\{\neg P,\neg Q,R\}$。

定义 公式 G 称为*恒真的*（或*有效的*），如果 G 在它的所有解释下都是真的；公式 G 称为*恒假的*（或*不可满足的*），如果 G 在它的所有解释下都是假的；公式 G 称为*可满足的*，如果它不是恒假的。

显然，G 是恒真的当且仅当$\neg G$ 是恒假的。

G 是可满足的当且仅当至少有一个解释 I，使 G 在 I 下为真。

若 G 是恒真的，则 G 是可满足的；反之不对。

如果公式 G 在解释 I 下是真的，则称 I *满足* G；如果 G 在解释 I 下是假的，则称 I *弄假* G。

判定问题 能否给出一个可行方法，对任意的公式，判定其是否是恒真公式。

因为一个命题公式的解释的数目是有穷的，所以命题逻辑的判定问题是可解的（可判定的，可计算的），亦即，命题公式的恒真，恒假性是可判定的。

定义 公式 G,H 说是*等价的*，记以 $G=H$，如果 G,H 在其任意解释 I 下，其真值相同。

显然，公式 G,H 等价的充要条件是公式 $G\leftrightarrow H$ 是恒真的。

两个公式间的等价关系，有反身性，对称性和传递性。

不难验证，下面的基本等价式是成立的。

1) $(G\leftrightarrow H)=(G\to H)\wedge(H\to G)$；

2) $(G\to H)=(\neg G\vee H)$；

3) $G\vee G=G, G\wedge G=G$； （等幂律）

4) $G\vee H=H\vee G, G\wedge H=H\wedge G$； （交换律）

5) $G\vee(H\vee S)=(G\vee H)\vee S, G\wedge(H\wedge S)=(G\wedge H)\wedge S$； （结合律）

6) $G\vee(G\wedge H)=G, G\wedge(G\vee H)=G$； （吸收律）

7) $G\vee(H\wedge S)=(G\vee H)\wedge(G\vee S), G\wedge(H\vee S)=(G\wedge H)\vee(G\wedge S)$；（分配律）

8) $G\vee 0=G, G\wedge 1=G$； （同一律）

9) $G\wedge 0=0, G\vee 1=1$； （零一律）

10) $\neg(G\vee H)=\neg G\wedge\neg H, \neg(G\wedge H)=\neg G\vee\neg H$。 （De Morgan 律）

定义 设 Q 是逻辑运算符号集合，若所有逻辑运算都能由 Q 中元素表示出来，而 Q 的任

意真子集无此性质，则称 Q 是一个完备集。

可以证明，$\{\neg,\wedge\}$，$\{\neg,\vee\}$ 都是完备集。

定义 设 P，Q 是两个命题，命题"P 与 Q 的否定"称为 P 与 Q 的与非式，记作 $P\uparrow Q$。$\uparrow$ 称作与非连结词。$P\uparrow Q$ 为真当且仅当 P，Q 不同时为真。

由定义可知：$P\uparrow Q=\neg(P\wedge Q)$

定义 设 P，Q 是两个命题，命题"P 或 Q 的否定"称为 P 与 Q 的或非式，记作 $P\downarrow Q$。$\downarrow$ 称作或非连结词。$P\downarrow Q$ 为真当且仅当 P，Q 同时为假。

由定义可知：$P\downarrow Q=\neg(P\vee Q)$

下面我们来说明 $\{\uparrow\}$ 是完备集。

$\neg P=P\uparrow P$

$P\vee Q=(P\uparrow P)\uparrow(Q\uparrow Q)$

$P\wedge Q=(P\uparrow Q)\uparrow(P\uparrow Q)$

读者可以自己证明 $\{\downarrow\}$ 也是完备集。

习　　题

1. 设命题 P，Q 的真值为 1，命题 R，S 的真值为 0，试确定下面命题的真值：

(1) $(P\wedge(Q\wedge R))\vee\neg((P\vee Q)\wedge(R\vee S))$

(2) $(\neg(P\wedge Q)\vee\neg R)\vee(((\neg P\wedge Q)\vee\neg R)\wedge S)$

(3) $(\neg(P\wedge Q)\vee\neg R)\vee((Q\leftrightarrow\neg P)\rightarrow(R\vee\neg S))$

(4) $(P\vee(Q\rightarrow(R\wedge\neg P)))\leftrightarrow(Q\vee\neg S)$

2. 证明下面的等价式：

(1) $(\neg P\wedge(\neg Q\wedge R))\vee(Q\wedge R)\vee(P\wedge R)=R$

(2) $P\rightarrow(Q\rightarrow P)=\neg P\rightarrow(P\rightarrow Q)$

(3) $P\rightarrow(Q\vee R)=(P\rightarrow Q)\vee(P\rightarrow R)$

(4) $(P\rightarrow Q)\wedge(R\rightarrow Q)=(P\vee R)\rightarrow Q$

§2　范　　式

我们将介绍命题公式的一种标准形式，即范式，两个命题公式是否等价及一个公式是否恒假(或恒真)的判定，都将由公式的范式来解决。

定义 原子或原子的否定称为文字。

例如，P、$\neg P$ 是文字。

定义 有限个文字的析取式称为一个子句；有限个文字的合取式称为一个短语。

特别，一个文字既可称为是一个子句，也可称为是一个短语。

例如，P，$P\vee Q$，$\neg P\vee Q$ 是子句，P，$P\wedge Q$，$\neg P\wedge\neg Q$ 是短语。

定义 有限个短语的析取式称为析取范式；有限个子句的合取式称为合取范式。

特别，一个文字既可称为是一个合取范式，也可称为是一个析取范式。一个子句，一个短语既可看做是合取范式，也可看做是析取范式。

例如，P、$P\wedge Q$，$P\vee Q$，$(P\wedge Q)\vee(\neg P\wedge\neg Q)$ 是析取范式。P、$P\wedge Q$，$P\vee Q$、$(P\vee Q)\wedge$

$(\neg P\vee R)$是合取范式。

定理 1　对于任意命题公式，都存在等价于它的析取范式和合取范式。

证明：对于公式 G，通过如下算法即可得出等价于 G 的范式：

步 1. 使用基本等价式，将 G 中的逻辑连结词$\rightarrow$，$\leftrightarrow$删除。

步 2. 使用$\neg(\neg H)=H$ 和 De Morgan 律，将 G 中所有的否定号$\neg$都放在原子之前。

步 3. 反复使用分配律，即可得到等价于 G 的范式。

例如，$G=(P\wedge(Q\rightarrow R))\rightarrow S$

$=\neg(P\wedge(\neg Q\vee R))\vee S$

$=\neg P\vee\neg(\neg Q\vee R)\vee S$

$=\neg P\vee(Q\wedge\neg R)\vee S$　　（析取范式）

$=\neg P\vee(Q\wedge\neg R)\vee(S\wedge(Q\vee\neg Q))$

$=\neg P\vee(Q\wedge\neg R)\vee(S\wedge Q)\vee(S\wedge\neg Q)$　　（析取范式）

$=(\neg P\vee S)\vee(Q\wedge\neg R)$

$=(\neg P\vee S\vee Q)\wedge(\neg P\vee S\vee\neg R)$　　（合取范式）

显然，给出一个公式 G，它的范式是不唯一的，能否有唯一的标准形式呢？有，这就是下面将要引进的主范式的概念。

定义　设 $P_1,\cdots,P_n$ 是 n 个不同原子，一个短语如果恰好包含所有这 n 个原子或其否定，且其排列顺序与 $P_1,\cdots,P_n$ 的顺序一致，则称此短语为关于 $P_1,\cdots,P_n$ 的一个极小项。

显然，共有 2^n 个不同的极小项。

例如，对原子 P,Q,R 而言，$P\wedge\neg Q\wedge R$，$\neg P\wedge\neg Q\wedge R$，$P\wedge Q\wedge R$ 都是极小项，但是，P，$\neg P\wedge Q$ 不是极小项，而$\neg P\wedge Q$ 对原子 P,Q 而言是极小项。

显然，对于 n 个原子 $P_1,\cdots,P_n$ 而言，其不同的解释共有 2^n 个，对于 $P_1,\cdots,P_n$ 的任一个极小项 m，2^n 个解释中，有且只有一个解释使 m 取 1 值。

例如，对 P,Q,R 而言，$\neg P\wedge Q\wedge\neg R$ 是极小项，解释$\{\neg P,Q,\neg R\}$使该极小项取 1 值，其他解释都使该极小项取 0 值。

如果将真值 1，0 看做是数，则每一个解释对应一个 n 位二进数。

假设使极小项 m 取 1 值的解释对应的二进数为 i，今后将 m 记为 m_i。

例如，对 P,Q,R 而言，$\neg P\wedge Q\wedge\neg R$ 是极小项，解释(0，1，0)使该极小项取 1 值，解释(0，1，0)对应的二进数是 2，于是$\neg P\wedge Q\wedge\neg R$ 记为 m_2。对 P,Q,R 而言，8 个极小项与其对应的解释如下：

极小项	解释	记法
$\neg P\wedge\neg Q\wedge\neg R$	000	m_0
$\neg P\wedge\neg Q\wedge R$	001	m_1
$\neg P\wedge Q\wedge\neg R$	010	m_2
$\neg P\wedge Q\wedge R$	011	m_3
$P\wedge\neg Q\wedge\neg R$	100	m_4
$P\wedge\neg Q\wedge R$	101	m_5
$P\wedge Q\wedge\neg R$	110	m_6
$P\wedge Q\wedge R$	111	m_7

因此，一般地，对 $P_1,\cdots,P_n$ 而言，2^n 个极小项为 $m_1,m_2,\cdots,m_{2^n-1}$。

下面，我们就给出主范式的概念。

定义 设命题公式 G 中所有不同原子为 $P_1,\cdots,P_n$，如果 G 的某个析取范式 G' 中的每一个短语，都是关于 $P_1,\cdots,P_n$ 的一个极小项，则称 G' 为 G 的**主析取范式**。恒假公式的主析取范式用 0 表示。

定理 2 对于命题公式 G，都存在等价于它的主析取范式。

证明：由定理 1 知，存在析取范式 G'，使得 $G=G'$。设 G 中所有不同原子为 $P_1,\cdots,P_n$，对于 G' 中每一个短语 G_i' 进行检查，如果 G_i' 不是关于 $P_1,\cdots,P_n$ 的极小项，则 G_i' 中必然缺少原子 $P_{j1},\cdots,P_{jk}$。因为

$$G_i' = G_i' \wedge (P_{j1} \vee \neg P_{j1}) \wedge \cdots \wedge (P_{jk} \vee \neg P_{jk})$$
$$= m_{i_1} \vee \cdots \vee m_{i_{2^k}}$$

于是将 G' 中非极小项 G_i' 化成了一些极小项之析取。对 G' 中其他非极小项也做如上处理，最后得等价于 G 的主析取范式 G^*。

在定理 2 的证明中，实际上已经给出了求公式的主析取范式的方法。

例如，$G=\neg(R\rightarrow P)\vee(Q\wedge(P\vee R))$

$=\neg(\neg R\vee P)\vee(Q\wedge P)\vee(Q\wedge R)$

$=(\neg P\wedge R)\vee(Q\wedge P)\vee(Q\wedge R)$

$=((\neg P\wedge R)\wedge(\neg Q\vee Q))\vee((Q\wedge P)\wedge(\neg R\vee R))\vee((Q\wedge R)\wedge(\neg P\vee P))$

$=(\neg P\wedge Q\wedge R)\vee(\neg P\wedge\neg Q\wedge R)\vee(P\wedge Q\wedge R)\vee(P\wedge Q\wedge\neg R)$

寻找与公式 G 等价的主析取范式，也可以通过真值表来做。

例如，公式 $G=(P\wedge Q)\vee(\neg P\wedge R)\vee(Q\wedge R)$ 的真值表如下：

P	Q	R	G
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

于是，G 的主析取范式为 $(\neg P\wedge\neg Q\wedge R)\vee(\neg P\wedge Q\wedge R)\vee(P\wedge Q\wedge\neg R)\vee(P\wedge Q\wedge R)$

下面我们来证明这种方法的正确性。

对于公式 G，用这种方法写出主析取范式 G'，若解释 I 使 G 取 1 值，而在 I 下取 1 值的唯一极小项写在 G' 中，故 G' 也取 1 值，若 I 使 G 取 0 值，而在 I 下取 1 的唯一极小项不在 G' 中且 I 弄假其它所有极小项，故 G' 取 0 值，所以 G' 是与 G 等价的主析取范式。

定理 3 设公式 G、H 是关于原子 $P_1,\cdots,P_n$ 的两个主析取范式。如果 G、H 不完全相同，则 G、H 不等价。

证明：因为 G、H 不完全相同，所以或者 G 中有一个极小项不在 H 中；或者反之。不妨设

极小项 m_i 在 G 中而不在 H 中。于是根据极小项的性质，二进制数 i 所对应的关于 $P_1,\cdots,P_n$ 的解释 I_i 使 m_i 取 1 值，从而使公式 G 取 1 值。I_i 使所有不是 m_i 的极小项取 0 值，从而使公式 H 取 0 值。故 G,H 不等价。

由定理 2，3 可得到如下定理：

定理 4　对于任意公式 G，存在唯一一个与 G 等价的主析取范式。

模仿主析取范式的概念不难给出主合取范式的概念，请读者作为练习，自己给出。

下面我们讨论，能否给出一个能行方法，即在有限步之内，判定一个命题公式是否恒真或恒假，这就是通常所说的判定问题。

用真值表法可以解决这一判定问题，但是这个方法即使是借助于计算机也是不好用的，下面我们讨论另一种方法。

引理　短语是恒假的当且仅当至少有一个原子及其否定（也称互补对）同时在此短语中出现。

证明：充分性，若有一个原子 P 及其否定 $\neg P$ 同时出现在短语中，则此短语有形式：

$$P \wedge \neg P \wedge \cdots$$

显然，不管是什么解释 I，$P\wedge\neg P$ 在 I 下取 0 值，于是此短语在 I 下取 0 值，故此短语恒假。

必要性，若短语恒假，而任意原子及其否定均不同时在短语中出现。那么，取这样的解释 I：指定带有否定号的原子取 0 值，不带否定号的原子取 1 值，显然，此短语在这个解释 I 下取 1 值，与此短语恒假矛盾。

定理 5　命题公式 G 是恒假的当且仅当在等价于它的析取范式中，每个短语均至少包含一个原子及其否定。

证明：设 G 的析取范式如下：

$$G = G_1 \vee \cdots \vee G_n$$

其中 G_i 是短语，$i=1,\cdots,n$。

显然，公式 G 恒假的充要条件是每个 G_i 恒假。再根据引理，此定理结论显然成立。

例如，判断公式 $G=(P\rightarrow Q)\wedge(Q\rightarrow R)\wedge(R\rightarrow P)$ 是否恒假。

解：
$$\begin{aligned}G &= (P\rightarrow Q)\wedge(Q\rightarrow R)\wedge(R\rightarrow P)\\ &= (\neg P\vee Q)\wedge(\neg Q\vee R)\wedge(\neg R\vee P)\\ &= ((\neg P\wedge\neg Q)\vee(Q\wedge\neg Q)\vee(\neg P\wedge R)\vee(Q\wedge R))\wedge(\neg R\vee P)\\ &= (\neg P\wedge\neg Q\wedge\neg R)\vee(Q\wedge\neg Q\wedge\neg R)\vee(\neg P\wedge R\wedge\neg R)\vee(Q\wedge R\wedge\neg R)\\ &\quad \vee(\neg P\wedge\neg Q\wedge P)\vee(Q\wedge\neg Q\wedge P)\vee(\neg P\wedge R\wedge P)\vee(Q\wedge R\wedge P)\end{aligned}$$

故公式 G 不是恒假的。

又如，判断公式 $G=(P\rightarrow Q)\wedge P\wedge\neg Q$ 是否恒假。

解：
$$\begin{aligned}G &= (P\rightarrow Q)\wedge P\wedge\neg Q\\ &= (\neg P\vee Q)\wedge P\wedge\neg Q\\ &= (\neg P\wedge P\wedge\neg Q)\vee(Q\wedge P\wedge\neg Q)\end{aligned}$$

故公式 G 是恒假的。

除了上面介绍的解决判定问题的方法外我们还可以用下面两种方法解决这个问题：

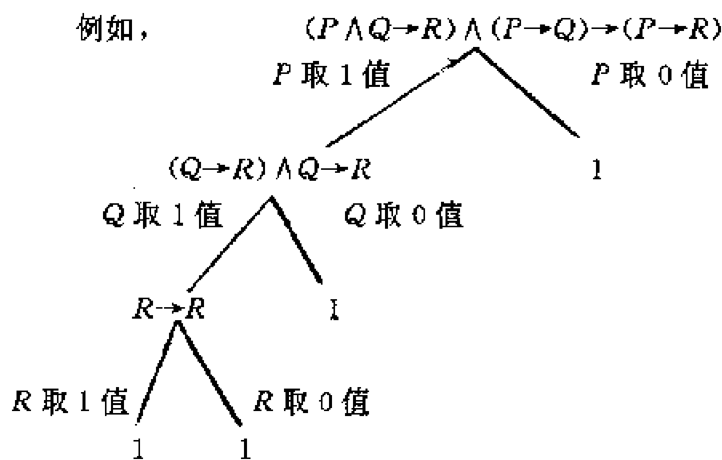
1. 把公式化成主析取范式，

公式恒假时，主析取范式没有极小项；公式恒真时，主析取范式有全部极小项。

2. 一种判定算法

对任给要判定的命题公式 G，设其中有原子 $P_1,P_2,\cdots,P_n$，令 P_1 取 1 值，求 G 的真值，或为 1，或为 0，或成为新公式 G_1 且其中只有原子 $P_2,\cdots,P_n$，再令 P_1 取 0 值，求 G 真值，如此继续，到最终只含 0 或 1 为止，若最终结果全为 1，则公式 G 恒真，若最终结果全为 0，则公式 G 恒假，若最终结果有 1，有 0，则是可满足的。

例如，



所以，此公式是恒真的。

习　　题

1. 试证明公式：

$((P\vee Q)\wedge\neg(\neg P\wedge(\neg Q\vee\neg R)))\vee(\neg P\wedge\neg Q)\vee(\neg P\wedge\neg R)$

是恒真公式。

2. 模仿主析取范式的概念，引进主合取范式的概念。并证明：对任意命题公式，存在唯一一个与其等价的主合取范式。

3. 证明：命题公式 G 是恒真的当且仅当在等价于它的合取范式中，每个子句均至少包含一个原子及其否定。

4. 试将下列公式化为析取范式和合取范式：

a) $P\wedge(P\rightarrow Q)$

b) $\neg(P\vee Q)\leftrightarrow(P\wedge Q)$

5. 试将下列公式化为主析取范式和主合取范式：

a) $P\rightarrow((P\rightarrow Q)\wedge\neg(\neg Q\vee\neg P))$；

b) $P\vee(\neg P\rightarrow(Q\vee(\neg Q\rightarrow R)))$。

6. 判断下列公式是恒真？恒假？可满足？

a) $(P\rightarrow(Q\wedge R))\wedge(\neg P\rightarrow(\neg Q\wedge\neg R))$；

b) $P\rightarrow(P\wedge(Q\rightarrow P))$；

c) $(Q\rightarrow P)\wedge(\neg P\wedge Q)$；

d) $(\neg P\vee\neg Q)\rightarrow(P\leftrightarrow\neg Q)$。

§3　公式的蕴涵

逻辑的一个重要功能是研究推理。固然，依靠等价关系可以进行推理。但是，进行推理时，不必一定要依靠等价关系，只需是蕴涵关系就可以了。

例如，若三角形等腰，则两底角相等，

　　这个三角形等腰，

　　所以，这个三角形两底角相等。

又如，若行列式两行成比例，则行列式值为0，

　　这个行列式两行成比例，

　　所以，这个行列式值为0。

上面两个例子的推理关系涵义不同，但依据的推理规则相同，推理形式为：

若P则Q，P，所以Q。

推理的正确性与命题P，Q涵义无关，只决定于逻辑形式，命题逻辑中用公式表示命题，命题间演绎推理关系，反映为公式间逻辑蕴涵关系。

定义　设G，H是两个公式。称H是G的*逻辑结果*（或称G*蕴涵*H），当且仅当对G，H的任意解释I，如果I满足G，则I也满足H，记作$G\Rightarrow H$。

注意：符号⇒和符号＝一样，它们都不是逻辑连结词，因此，$G=H$，$G\Rightarrow H$也不是公式。

⇒是一种部分序关系。

不难证明，公式G蕴涵公式H的充要条件是：公式$G\rightarrow H$是恒真的。

例如，$(P\wedge Q)\Rightarrow P$，$(P\Rightarrow Q)\Rightarrow Q$

定义　设$G_1,\cdots,G_n,H$是公式。称H是$G_1,\cdots,G_n$的*逻辑结果*（或称$G_1,\cdots,G_n$*共同蕴涵*H），当且仅当公式$G_1\wedge\cdots\wedge G_n$蕴涵$H$。

显然，公式H是$G_1,\cdots,G_n$的逻辑结果的充要条件是：公式$((G_1\wedge\cdots\wedge G_n)\rightarrow H)$是恒真的。

例如，P，$P\rightarrow Q$共同蕴涵Q。

定理1　如果$H_1,\cdots,H_m$，P共同蕴涵公式Q，则$H_1,\cdots,H_m$共同蕴涵公式$P\rightarrow Q$。

证明：因为$(H_1\wedge\cdots\wedge H_m\wedge P)\Rightarrow Q$，所以公式$(H_1\wedge\cdots\wedge H_m\wedge P)\rightarrow Q$是恒真的。利用下面的基本等价公式：

$$P_1\rightarrow(P_2\rightarrow P_3)=(P_1\wedge P_2)\rightarrow P_3$$

于是，$(H_1\wedge\cdots\wedge H_m\wedge P)\rightarrow Q=(H_1\wedge\cdots\wedge H_m)\rightarrow(P\rightarrow Q)$。故$(H_1\wedge\cdots\wedge H_m)\rightarrow(P\rightarrow Q)$是恒真的。所以$H_1,\cdots,H_m$共同蕴涵$P\rightarrow Q$。

例如，因为公式$P\rightarrow Q$，$Q\rightarrow R$，P共同蕴涵R，所以$P\rightarrow Q$，$Q\rightarrow R$共同蕴涵$P\rightarrow R$。

定义　设S是一个命题公式的集合（前提集合）。从S推出公式G的一个*演绎*是公式的一个有限序列：

$$G_1,\cdots,G_t$$

其中，G_i或者属于S，或者是某些$G_j(j<i)$的逻辑结果。并且G_t就是G。我们称公式G为此演绎的*逻辑结果*，或称从S*演绎出*G。有时也记为$S\Rightarrow G$。

例如，设$S=\{P\vee Q,Q\rightarrow R,P\rightarrow M,\neg M\}$则下面的公式序列

$$\neg M,P\rightarrow M,\neg P,P\vee Q,Q,Q\rightarrow R,R$$

就是从 S 推出 R 的一个演绎。

从演绎的定义知，演绎中仅仅使用了蕴涵的概念，也就是说，演绎是在蕴涵概念下进行的。下面给出的定理说明，演绎也是一种蕴涵，只不过是换了一种形式。

引理 设 G,H_1,H_2 是公式。如果 G 蕴涵 H_1，G 蕴涵 H_2，则 G 蕴涵 $H_1 \wedge H_2$。

证明：任取 G,H_1,H_2 的一个解释 I。若 I 满足 G，由假设知，I 满足 H_1，I 满足 H_2，故 I 满足 $H_1 \wedge H_2$。由 I 的任意性，所以 $G \Rightarrow (H_1 \wedge H_2)$。

定理 2 设 S 是公式集合，G 是一个公式。于是，从 S 演绎出 G 的充要条件是 G 是 S 的逻辑结果。

证明：必要性，设从 S 演绎出 G，令

$$G_1, \cdots, G_k$$

是这个演绎。

对任意 $G_i(i=1,\cdots,k)$，往证 G_i 是 S 的逻辑结果。对 i 用归纳法。

当 $i=1$ 时，因 $G_1 \in S$，显然

$$G_1 \wedge \cdots \to G_1$$

是恒真公式，故 $S \Rightarrow G_1$，即 G_1 是 S 的逻辑结果。

设 $i<n$ 时，命题成立。

当 $i=n$ 时，若 $G_n \in S$，则 $S \Rightarrow G_n$，归纳法完成。

若 G_n 是某些 $G_j(j<n)$ 的逻辑结果，不妨设

$$(G_{j1} \wedge \cdots \wedge G_{jh}) \Rightarrow G_n \tag{1}$$

其中 $j1,\cdots,jh$ 都小于 n。

由归纳假设知，$S \Rightarrow G_{jm}$，$m=1,\cdots,h$。由引理知：

$$S \Rightarrow (G_{j1} \wedge \cdots \wedge G_{jh}) \tag{2}$$

根据(1)，(2)式及蕴涵关系的传递性，得

$$S \Rightarrow G_n$$

即 G_n 是 S 的逻辑结果，归纳完成。

充分性，若 G 是 S 的逻辑结果，由演绎的定义知，G 是如下演绎：

$$G_1, \cdots, G_k, G$$

的逻辑结果，其中 $G_1,\cdots,G_k$ 是 S 中所有公式。

定理 3 设 S 是前提公式集合，G,H 是两个公式。如果从 $S \cup \{G\}$ 可演绎出 H，则从 S 可演绎出 $G \to H$。

证明：因为从 $S \cup \{G\}$ 可演绎出 H，由定理 2 知，H 是 $S \cup \{G\}$ 的逻辑结果。亦即

$$(G_1 \wedge \cdots \wedge G_k \wedge G) \Rightarrow H$$

其中 $G_1,\cdots,G_k$ 是 S 中所有公式。

由定理 1 知：

$$(G_1 \wedge \cdots \wedge G_k) \Rightarrow (G \to H)$$

即 $G \to H$ 是 S 的逻辑结果，再由定理 2 知，从 S 可演绎出 $G \to H$。

在命题逻辑中进行演绎，要不断地使用已知的蕴涵公式，过去我们知道的基本等价式当然可以当做两个蕴涵式使用，因为 $G=H$ 的充要条件是 $(G \Rightarrow H)$ 和 $(H \Rightarrow G)$（读者不难自己证明）。下面我们再给出一些基本蕴涵式，以便在演绎时使用，这些基本蕴涵式的正确性，留给读者自己证明。

一些基本蕴涵式：

1. $P\wedge Q\Rightarrow P$
2. $P\wedge Q\Rightarrow Q$
3. $P\Rightarrow P\vee Q$
4. $Q\Rightarrow P\vee Q$
5. $\neg P\Rightarrow(P\rightarrow Q)$
6. $Q\Rightarrow(P\rightarrow Q)$
7. $\neg(P\rightarrow Q)\Rightarrow P$
8. $\neg(P\rightarrow Q)\Rightarrow\neg Q$
9. $P,Q\Rightarrow P\wedge Q$
10. $\neg P,P\vee Q\Rightarrow Q$
11. $P,P\rightarrow Q\Rightarrow Q$
12. $\neg Q,P\rightarrow Q\Rightarrow\neg P$
13. $P\rightarrow Q,Q\rightarrow R\Rightarrow P\rightarrow R$
14. $P\vee Q,P\rightarrow R,Q\rightarrow R\Rightarrow R$

至此，给出两个公式 G,H，证明 G 蕴涵 H，我们有如下几种方法：

1. 真值表法；
2. 证 $G\rightarrow H$ 是恒真公式；
3. 利用一些基本等价式及蕴涵式进行推导；
4. 任取解释 I，若 I 满足 G、往证 I 满足 H；
5. 反证法，设结论假，往证前提假。

若给出前提集合 $S=\{G_1,\cdots,G_k\}$，公式 G，证明 $S\Rightarrow G$ 有如下两种方法：

1. $G_1\wedge\cdots\wedge G_k\Rightarrow G$

2. 形式演绎法：根据一些基本等价式和基本蕴涵式，从 S 出发，演绎出 G，在演绎过程中我们遵循以下三条规则：

规则 1. 可随便使用前提。（根据演绎定义）

规则 2. 可随便使用前面演绎出的某些公式的逻辑结果。（根据演绎的定义）

规则 3. 如果需要演绎出的公式是 $P\rightarrow Q$ 的形式，则我们可将 P 做为附加前提使用，而力图去演绎出 Q。（根据定理 3）

例如，证明$\{(P\vee Q),(P\rightarrow R),(Q\rightarrow S)\}\Rightarrow S\vee R$

1. $P\vee Q$	规则 1
2. $\neg P\rightarrow Q$	规则 2，根据 1
3. $Q\rightarrow S$	规则 1
4. $\neg P\rightarrow S$	规则 2，根据 2，3
5. $\neg S\rightarrow P$	规则 2，根据 4
6. $P\rightarrow R$	规则 1
7. $\neg S\rightarrow R$	规则 2，根据 5，6
8. $S\vee R$	规则 2，根据 7。

又如，证明$\{P\rightarrow(Q\rightarrow S),\neg R\vee P,Q\}\Rightarrow R\rightarrow S$

1. $\neg R\vee P$	规则 1

2. R　　规则 3
3. P　　规则 2，根据 1，2
4. $P \to (Q \to S)$　　规则 1
5. $Q \to S$　　规则 2，根据 3，4
6. Q　　规则 1
7. S　　规则 2，根据 5，6
8. $R \to S$　　规则 3，根据 2，7

再如，若厂方拒绝增加工资，则罢工不会停止，除非罢工超过一年并且工厂经理辞职。问：如果厂方拒绝增加工资，而罢工又刚刚开始，罢工是否能停止？

令 P：厂方拒绝增加工资；

Q：罢工停止；

R：工厂经理辞职；

S：罢工超过一年。

于是，

G_1：$(P \wedge \neg(R \wedge S)) \to \neg Q$

G_2：P

G_3：$\neg S$

H：$\neg Q$

我们要证明：H 是 $\{G_1, G_2, G_3\}$ 的逻辑结果。

1. $\neg S$　　规则 1
2. $\neg S \vee \neg R$　　规则 2，根据 1
3. $\neg(R \wedge S)$　　规则 2，根据 2
4. P　　规则 1
5. $P \wedge \neg(R \wedge S)$　　规则 2，根据 3，4
6. $(P \wedge \neg(R \wedge S)) \to \neg Q$　　规则 1
7. $\neg Q$　　规则 2，根据 5，6

亦即，罢工不会停止。

习　　题

1. 设 $S = \{G_1, \cdots, G_n\}$ 是命题公式集合。试求出从 S 出发演绎出的所有命题公式。

   提示：考虑 $G_1 \wedge \cdots \wedge G_n$ 的主合取范式。

2. 证明：两个公式之间的蕴涵关系具有反身性、反对称性和传递性。

3. 证明：若前提集合 S 中的公式都是恒真的，G 是从 S 出发的一个演绎的逻辑结果，则 G 必是恒真公式。

4. 设 $G_1, \cdots, G_n$ 是公式。证明：从 $\{G_1, \cdots, G_n\}$ 出发可演绎出公式 G 的充要条件是从 $\{G_1, \cdots, G_n, \neg G\}$ 出发可演绎出公式 $(R \wedge \neg R)$。其中 R 为任意公式。

5. 证明下列蕴涵式：

   a) $(P \wedge Q) \Rightarrow (P \to Q)$

   b) $P \Rightarrow (Q \to P)$

c) $(P\to(Q\to R))\Rightarrow(P\to Q)\to(P\to R)$

d) $P\to Q\Rightarrow P\to(P\land Q)$

e) $(P\to Q)\to Q\Rightarrow P\lor Q$

f) $((P\lor\neg P)\to Q)\to((P\lor\neg P)\to R)\Rightarrow(Q\to R)$

g) $(Q\to(P\land\neg P))\to(R\to(P\land\neg P))\Rightarrow(R\to Q)$

6. 证明$\{C\lor D,(C\lor D)\to\neg H,\neg H\to(A\land\neg B),(A\land\neg B)\to(R\lor S)\}$共同蕴涵$R\lor S$。

7. 证明$\{P\lor Q,Q\to R,P\to M,\neg M\}$共同蕴涵$R\land(P\lor Q)$。

8. 证明$\{\neg P\lor Q,\neg Q\lor R,R\to S\}$共同蕴涵$P\to S$。

第三章　一阶逻辑

§1　谓词与量词

命题逻辑研究的基本元素是命题。命题是有真假意义的一句话，而对这句话的结构和成分是不考虑的。因此，用这样简单的手段，很多思维过程不能在命题逻辑中表达出来。

例如，逻辑学中著名的三段论：

凡人必死

张三是人

张三必死

在命题逻辑中就无法表示这种推理过程。

因为，如果用 P 代表"凡人必死"这个命题，Q 代表"张三是人"这个命题，R 代表"张三必死"这个命题，则按照三段论，R 应该是 P 和 Q 的逻辑结果。但是，在命题逻辑中，R 却不是 P 和 Q 的逻辑结果，因为公式

$$P \wedge Q \rightarrow R$$

显然不是恒真的，解释 $\{P, Q, \neg R\}$ 就能弄假上面的公式。

发生这种情况的原因是：命题逻辑中描述出来的三段论，即 $P \wedge Q \rightarrow R$，使 R 成为一个与 P，Q 无关的独立命题。因此，取解释时，可将 P，Q 取真，R 取假，从而弄假公式 $P \wedge Q \rightarrow R$。但是，实际上命题 R 是和命题 P，Q 有关系的，只是这种关系在命题逻辑中无法表示。为了表示出这三个命题的内在关系，我们需要引进谓词的概念。

定义　设 D 是非空个体名称集合。定义在 D^n 上取值于 $\{1,0\}$ 上的 n 元函数，称为 *n 元命题函数*或 *n 元谓词*。其中 D^n 表示集合 D 的 n 次笛卡尔乘积。

一般地，一元谓词描述个体的性质，二元或多元谓词描述两个或多个个体间的关系。0 元谓词中无个体，理解为就是命题，这样，一阶逻辑包括命题逻辑。

下面我们举一个谓词的例子：

令 $G(x, y)$："x 高于 y"，于是，$G(x, y)$ 是一个二元谓词。将 x 代以个体"张三"，y 代以个体"李四"，则 G(张三，李四)就是命题："张三高于李四"。随便将 x，y 代以确定的个体，由 $G(x, y)$ 都能得到一个命题。但是，$G(x, y)$ 不是命题，而是一个命题函数即谓词。

于是，用谓词的概念可将三段论做如下的符号化：令

$H(x)$ 表示"x 是人"

$M(x)$ 表示"x 必死"

则三段论的三个命题表示如下：

P：$H(x) \rightarrow M(x)$

Q：H(张三)

R：M(张三)

那么，在命题逻辑的基础上，仅仅引进谓词的概念是否就可以了呢？下面的例子说明，仅有谓词还是不够的。例如我们想得到"命题"P 的否定"命题"，应该就是"命题"$\neg P$。但是，

$$\neg P = \neg(H(x) \to M(x))$$
$$= \neg(\neg H(x) \vee M(x))$$
$$= H(x) \wedge \neg M(x)$$

亦即，“命题”P 的否定“命题”是“所有人都不死”。这和人们日常对命题“所有人都必死”的否定的理解，相差得实在太远了。

其原因在于，命题 P 的确切意思应该是：“对任意 x，如果 x 是人，则 x 必死”。但是

$$H(x) \to M(x)$$

中并没有确切的表示出“对任意 x”这个意思，亦即 $H(x) \to M(x)$ 不是一个命题。因此，在谓词逻辑中除引进谓词外，还需要引进“对任意 x”这个语句，及其对偶的语句“存在一个 x”。

定义　语句“对任意 x”称为*全称量词*，记以 $\forall x$；语句“存在一个 x”称为*存在量词*，记以 $\exists x$。

这时，命题 P 就可确切地符号化如下：

$$\forall x(H(x) \to M(x))$$

命题 P 的否定命题为：

$$\neg P = \neg(\forall x(H(x) \to M(x)))$$
$$= \exists x(H(x) \wedge \neg M(x))$$

亦即“有一个人是不死的”。这个命题确实是“所有人都要死”的否定。

有了谓词和量词的概念，就可以建立起一阶逻辑了。三段论的三个命题，在一阶逻辑中是如下这样表示的：

P：$\forall x(H(x) \to M(x))$

Q：H(张三)

R：M(张三)

以后可以证明：在一阶逻辑中，R 是 P 和 Q 的逻辑结果。

设 $G(x)$ 是一元谓词，任取 $x_0 \in D$，则 $G(x_0)$ 是一个命题，于是 $\forall xG(x)$ 是这样一个命题“对任意 $x \in D$，都有 $G(x)$”。故对命题 $\forall xG(x)$ 的真值做如下规定是自然的。

$\forall xG(x)$ 取 1 值 $\Leftrightarrow$ 对任意 $x \in D$，$G(x)$ 都取 1 值；

$\forall xG(x)$ 取 0 值 $\Leftrightarrow$ 有一个 $x_0 \in D$，使 $G(x_0)$ 取 0 值。

类似地，$\exists xG(x)$ 是命题“存在一个 $x_0 \in D$，使得 $G(x_0)$ 成立”。对命题 $\exists xG(x)$ 的真值规定如下：

$\exists xG(x)$ 取 1 值 $\Leftrightarrow$ 有一个 $x_0 \in D$，使 $G(x_0)$ 取 1 值；

$\exists xG(x)$ 取 0 值 $\Leftrightarrow$ 对所有 $x \in D$，$G(x)$ 都取 0 值。

通过这个规定可以看出，当 $D=\{x_0, x_1, \cdots\}$ 是可数集合时，

$\forall xG(x)$ 等价于 $G(x_1) \wedge G(x_2) \wedge \cdots$

$\exists xG(x)$ 等价于 $G(x_1) \vee G(x_2) \vee \cdots$

对于一个谓词，如果其中每一个变量都在一个量词作用之下。则它就不再是命题函数，而是一个命题了。但是，这种命题和命题逻辑中的命题毕竟有所不同。因为终归这种命题里还有变量，当然这种变量和命题函数中的变量还有区别。

因此，使用量词时应注意以下几个问题：

1. 量词的论域，即 D 中都有哪些元素；

2. 在多重量词时，应注意量词的顺序；

3. 量词的作用范围。

定义 在一个由谓词，量词，逻辑连结词，括号组成的有意义的符号串（实际是指下一节将严格定义的公式）中，变量的出现说是约束的，当且仅当它出现在使用这个变量的量词范围之内；变量的出现说是自由的，当且仅当这个出现不是约束的。

例如，$\exists x(P(x,y)\rightarrow Q(x,z))\vee R(x)$。从左向右算起，变量 x 的第一，第二次出现是约束的，第三次出现是自由的；变量 y,z 的出现是自由的。

定义 变量说是约束的，如果至少一个它的出现是约束的；变量说是自由的，如果至少一个它的出现是自由的。

由定义可以看出一个变量可以既是约束变量又是自由变量。

例如，上例中的 x 既是约束变量，又是自由变量；y,z 只是自由变量。

显然，$\exists xG(x)$ 与 $\exists yG(y)$ 的真值一样，$\forall xG(x)$ 与 $\forall yG(y)$ 的真值一样，亦即，一阶逻辑中的命题的真值，与命题中的约束变量的记法无关。这就引出了一阶逻辑中的改名规则。

在由谓词，量词，逻辑连结词，括号组成的有意义的符号串（实际是下节定义的公式）中，我们可将其中出现的约束变量改为另一个约束变量，这种改名必须在量词作用区域内各处以及该量词符号中实行，并且改成的新约束变量要有别于改名区域中的所有其它变量。显然改名规则不改变原符号串的真值。

例如，对于 $\forall x(P(x,y)\vee Q(x,z))$，可改名为 $\forall u(P(u,y)\vee Q(u,z))$。但下面的改名都是不对的：

(1) $\forall u(P(u,y)\vee Q(x,z))$

(2) $\forall x(P(u,y)\vee Q(u,z))$

(3) $\forall u(P(x,y)\vee Q(x,z))$

(4) $\forall y(P(y,y)\vee Q(y,z))$

(5) $\forall z(P(z,y)\vee Q(z,z))$

因此，在一阶逻辑中的一个表达式里，我们总可以通过改名规则，使得该表达式中所有的约束变量都不是自由变量，于是所有的自由变量也都不是约束变量了。以后的讨论，我们总是在这种假定下进行。

习　题

1. 设下面所有谓词的定义域都是 $\{a,b,c\}$。试将下面谓词公式中的量词消除，写成与之等价的命题公式。

a) $\forall xR(x)\wedge\exists xS(x)$

b) $\forall x(P(x)\rightarrow Q(x))$

c) $\forall x\neg P(x)\vee\forall xP(x)$

2. 指出下列命题的真值：

a) $\forall x(P\rightarrow Q(x))\vee R(e)$，

其中，P："$3>2$"，$Q(x)$："$x\leq 3$"，$R(x)$："$x>5$"，e：3，定义域 $S=\{-2,3,6\}$。

b) $\exists x(P(x)\rightarrow Q(x))$，

其中，$P(x)$："$x>3$"，$Q(x)$："$x=4$"，定义域 $S=\{2\}$。

§2 公 式

在本节中，我们将对一阶逻辑中关于谓词的表达式形式化，亦即引进公式的概念、并引进关于公式的恒真，恒假，等价，蕴涵等最基本的概念。

在形式化中，我们将使用如下四种符号：

1. 常量符号：用小写英文字母 $a,b,c,\cdots$ 表示，当个体名称集合 D 给出时，它可以是 D 中某个元素。

2. 变量符号：用小写英文字母 $x,y,z,\cdots$ 表示，当个体名称集合 D 给出时，D 中任意元素可代入变量符号。

3. 函数符号：用小写英文字母 $f,g,\cdots$ 表示，当个体名称集合 D 给出时，n 元函数符号 $f(x_1,\cdots,x_n)$ 可以是 D^n 到 D 的任意一个映射。

4. 谓词符号：用大写英文字母 $P,Q,R,\cdots$ 表示，当个体名称集合 D 给出时，n 元谓词符号 $P(x_1,\cdots,x_n)$ 可以是 D^n 上的任意一个谓词。

定义 一阶逻辑中的项，被递归定义为：

1）常量符号是项；

2）变量符号是项；

3）若 $f(x_1,\cdots,x_n)$ 是 n 元函数符号，$t_1,\cdots,t_n$ 是项，则 $f(x_1,\cdots,x_n)$ 是项；

4）所有项都是有限次使用 1)，2)，3)生成的符号串。

定义 若 $P(x_1,\cdots,x_n)$ 是 n 元谓词符号，$t_1,\cdots,t_n$ 是项，则 $P(x_1,\cdots,x_n)$ 是原子。

定义 一阶逻辑中的公式，被递归定义如下：

1）原子是公式；

2）若 G,H 是公式，则 $(\neg G)$，$(G\vee H)$，$(G\wedge H)$，$(G\rightarrow H)$，$(G\leftrightarrow H)$ 是公式；

3）若 G 是公式，x 是 G 中的自由变量，则 $\forall xG$，$\exists xG$ 是公式；

4）所有公式都是有限次使用 1)～3)生成的符号串。

由于公式是由常量符号，变量符号，函数符号，谓词符号通过逻辑连结词和量词（当然还有括号）连结起来的抽象符号串，所以若不对它们（常量符号，变量符号，函数符号，谓词符号）给以具体解释，则公式是没有实在意思的。所谓给公式以解释，就是将公式中的常量符号指为常量，函数符号指为函数，谓词符号指为谓词。

定义 一阶逻辑中公式 G 的一个解释 I，是由非空区域 D 和对 G 中常量符号，函数符号，谓词符号按下列规则进行的一组指定组成：

1. 对每个常量符号，指定 D 中一个元素；

2. 对每个 n 元函数符号，指定一个函数，即指定 D^n 到 D 的一个映射；

3. 对每个 n 元谓词符号，指定一个谓词，即指定 D^n 到 $\{0,1\}$ 的一个映射。

今后我们对讨论的公式做如下规定：公式中无自由变量，或将自由变量看做常量。

显然，对任意公式 G，如果给出 G 的一个解释 I，则 G 在 I 下有一个真值，记作 $T_I(G)$。

例如，给出如下两个公式：

1）$G=\exists x(P(f(x))\wedge Q(x,f(a)))$

2）$H=\forall x(P(x)\wedge Q(x,a))$

给出如下的解释 I：

$D=\{2,3\}$

a
2

$f(2)$	$f(3)$
3	2

$P(2)$	$P(3)$	$Q(2,2)$	$Q(2,3)$	$Q(3,2)$	$Q(3,3)$
0	1	1	1	0	1

于是，$T_I(G)=T_I((P(f(2))\wedge Q(2,f(2)))\vee(P(f(3))\wedge Q(3,f(2))))$

$=T_I((P(3)\wedge Q(2,3))\vee(P(2)\wedge Q(3,3)))$

$=(1\wedge 1)\vee(0\wedge 0)$

$=1$

$T_I(H)=T_I(P(2)\wedge Q(2,2)\wedge P(3)\wedge Q(3,2))$

$=0\wedge 1\wedge 1\wedge 0$

$=0$

定义 公式 G 称为可满足的，如果存在解释 I，使 G 在 I 下取 1 值，简称 I 满足 G。若 I 不满足 G，则简称 I 弄假 G。

定义 公式 G 称为是恒假的（或不可满足的），如果不存在解释 I 满足 G；公式 G 称为恒真的，如果 G 的所有解释 I 都满足 G。

定义 公式 G,H 称为等价，记以 $G=H$，如果公式 $G\leftrightarrow H$ 是恒真的。

由定义显然可以看出：公式 G,H 等价的充要条件是：对 G,H 的任意解释 I，G,H 在 I 下的真值相同。

因为对任意公式 G,H，在解释 I 下，G,H 就是两个命题，所以命题逻辑中给出的 10 组基本等价式，在一阶逻辑中仍然成立。

定义 设 G,H 是公式，称 G 蕴涵 H，或 H 是 G 的逻辑结果，如果公式 $G\rightarrow H$ 是恒真的，并记以 $G\Rightarrow H$。

显然，对任意两个公式 G,H，G 蕴涵 H 的充要条件是：对任意解释 I，若 I 满足 G，则 I 必满足 H。

同样，命题逻辑中的 14 组基本蕴涵式仍成立。

现在，我们再回到三段论上来。

令 $G_1=\forall x(H(x)\rightarrow M(x))$

$G_2=H(a)$

$H=M(a)$

我们将证明：H 是 $G_1\wedge G_2$ 的逻辑结果。

因为，设 I 是 G_1,G_2,H 的一个解释（I 指定 a 为张三），且 I 满足 $G_1\wedge G_2$，即 I 满足

$$\forall x(H(x)\rightarrow M(x))\wedge H(a)$$

所以，I 满足 $M(a)$。

否则，令 $M(a)$ 在 I 下为假，而 $H(a)$ 在 I 下为真，于是 $H(a)\rightarrow M(a)$ 在 I 下为假，故 $\forall x(H(x)\rightarrow M(x))$ 在 I 下为假，矛盾！

故 $M(a)$ 在 I 下为真命题，而 I 指定 a 为“张三”，故 M(张三)为真命题。

顺便提一句，由于一阶逻辑中的恒真（恒假）公式，要求所有解释 I 都满足（弄假）该公式。而解释 I 依赖于一个非空集合 D。由于集合 D 可以是无穷集合，而集合 D 的“数目”也可能是

无穷多个，因此，所谓公式的"所有"解释，实际上是无法考虑的。这就使得一阶逻辑中公式的恒真，恒假性的判断变得异常困难。1936 年 Church 和 Turing 分别独立地证明了：对于一阶逻辑，判定问题是不可解的。

幸好，一阶逻辑是半可判定的，亦即，如果一阶逻辑中的公式是恒真的，则有算法在有限步之内检验出这个公式的恒真性。如果该公式不是恒真的(当然也不是恒假的)，则无法在有限步内判定这个事实。从 Thurch 和 Turing 的结果看，这也许是我们所能期望的最好结果了。

设 $G(x)$ 是一元谓词符号，若公式 $\forall xG(x)$ 是恒真公式，则这件事实可被叙述为如下的一个真命题：对任意一元谓词 $G(x)$，命题 $\forall xG(x)$ 都是真的。

但是，如果想把这个命题加以否定，则在一阶逻辑中是办不到的。因为：

1) 这个命题的否定，应该是如下命题：有一个一元谓词 $G(x)$，使得命题 $\forall xG(x)$ 是假的。

2) 公式 $\forall xG(x)$ 的否定是公式 $\neg(\forall xG(x))$。而后一个公式表示的命题是：公式 $\forall xG(x)$ 是恒假的，亦即，对任意一元谓词 $G(x)$，命题 $\forall xG(x)$ 都是假的。

可以看到，1)和 2)所表示出的事实相差得太远了。发生这件事的原因是：用"公式 $\forall xG(x)$ 是恒真的"来表达命题"对任意一元谓词 $G(x)$，命题 $\forall xG(x)$ 都是真的"是不确切的。确切地，后一个命题，应该用"公式 $\forall G(\forall xG(x))$ 是恒真的"来表达。

这个公式中，不仅有关于个体变量 x 的量词，而且有关于谓词变量(即谓词符号，亦即原子)的量词。由这样的公式组成的系统就称为高阶逻辑。高阶逻辑中，不仅判定问题不可解，甚至连一个完备的公理系统都没有。关于高阶逻辑的讨论已超出本书的范围，有兴趣的读者，可阅读有关专著。

习 题

1. 设 I 是如下一个解释：

$D=\{a,b\}$

$P(a,a)$	$P(a,b)$	$P(b,a)$	$P(b,b)$
1	0	0	1

试确定下列公式在 I 下的真值：

a) $\forall x\exists yP(x,y)$；

b) $\forall x\forall yP(x,y)$；

c) $\exists x\forall yP(x,y)$；

d) $\exists x\neg P(a,y)$；

e) $\forall x\forall y(P(x,y)\to P(y,x))$；

f) $\forall xP(x,x)$

2. 设 $G=\exists xP(x)\to\forall xP(x)$。

a) 若解释 I 的非空区域 D 包含仅仅一个元素，则 G 在 I 下取 1 值。

b) 设 $D=\{a,b\}$，试找出一个 D 上的解释 I，使 G 在 I 下取 0 值。

3. 设 I 是如下一个解释：

$D=\{3,2\}$

a	b	$f(3)$	$f(2)$	$P(3,3)$	$P(3,2)$	$P(2,3)$	$P(2,2)$
3	2	2	3	1	1	0	0

试求出下列公式在 I 下的真值：

a) $P(a,f(a))\wedge P(b,f(b))$；

b) $\forall x\exists yP(y,x)$；

c) $\forall x\forall y(P(x,y)\to P(f(x),f(y)))$

4. 设 $G_1=\forall x(P(x)\to Q(x))$，$G_2=\neg Q(a)$，证明：$\neg P(a)$是 G_1 和 G_2 的逻辑结果。

5. 试证明下列等价式或蕴涵式，其中 $A(x)$，$B(x)$表示含自由变量 x 的公式，A、B 表示不含变量 x(不论是自由的还是约束的)的公式。

a) $(\forall xA(x)\to B)=(\exists x(A(x)\to B))$；

b) $(\exists xA(x)\to B)=\forall x(A(x)\to B)$；

c) $(A\to\forall xB(x))=\forall x(A\to B(x))$；

d) $(A\to\exists xB(x))=\exists x(A\to B(x))$；

e) $\exists x(A(x)\to B(x))=(\forall xA(x)\to\exists xB(x))$；

f) $(\exists xA(x)\to\forall xB(x))\Rightarrow\forall x(A(x)\to B(x))$；

g) $(\forall xA(x)\vee\forall xB(x))\Rightarrow\forall x(A(x)\vee B(x))$；

h) $\exists x(A(x)\wedge B(x))\Rightarrow(\exists xA(x)\wedge\exists x(B(x))$。

6. 若$\exists x(P(x)\wedge Q(x))$，$\exists y(P(y)\wedge R(y))$在某解释 I 下取 1 值，则$\exists z(Q(z)\wedge R(z))$是否在 I 下取 1 值？其中 P,Q,R 的定义域中有两个元素。若将存在量词都换为全称量词，结果怎样？

§3 范　　式

在命题逻辑中，我们引进过公式的标准形式，即范式。因为一个公式，在等价意义下，可以有各种不同的表示，因此，公式的标准表示形式就是一个有意义的问题。在命题逻辑中，范式的重要作用我们已经知道，范式在一阶逻辑中有同样重要的作用，本节我们讨论一阶逻辑中公式的两种标准形式。

定义　一阶逻辑中公式 G 称为*前束范式*，如果 G 有如下形状：

$$Q_1x_1\cdots Q_nx_nM$$

其中 Q_ix_i 或者是$\forall x_i$，或者是$\exists x_i$，$i=1,\cdots,n$，M 是不含量词的公式，$Q_1x_1\cdots Q_nx_n$ 称为首标，M 称为*母式*。

例如，$\forall x\forall y\exists z(P(x,y)\to Q(x,z))$

$\exists x\exists y\exists zP(x,y,z)$

等等，就是前束范式。

引理 1　设 G 是公式，其中自由变量有且仅有一个 x，记以 $G(x)$，H 是不含变量 x 的公式，于是有：

1)　$\forall x(G(x)\vee H)=\forall xG(x)\vee H$

1′)　$\exists x(G(x)\vee H)=\exists xG(x)\vee H$

2)　$\forall x(G(x)\wedge H)=\forall xG(x)\wedge H$

2′)　$\exists x(G(x)\wedge H)=\exists xG(x)\wedge H$

3)　$\neg(\forall xG(x))=\exists x(\neg G(x))$

4)　$\neg(\exists xG(x))=\forall x(\neg G(x))$

证明：我们只证明1)和4)。

1) 设I是$G(x)$和H的一个解释。若$\forall x(G(x)\vee H)$在I下取1值，则在I下，对任意$x\in D$，$G(x)\vee H$都是真命题。若H是真命题，则$\forall xG(x)\vee H$是真命题；若H是假命题，则必然是对每个$x\in D$，$G(x)$都是真命题，故$\forall xG(x)$取1值。所以$\forall xG(x)\vee H$在I下取1值。

若$\forall x(G(x)\vee H)$在I下取0值，则必有一个$x_0\in D$，使$G(x_0)\vee H$在I下取0值。故$G(x_0)$为假命题，H为假命题。所以$\forall xG(x)$取0值。从而$\forall xG(x)\vee H$在I下取0值。

4) 若I满足$\neg(\exists xG(x))$，则I弄假$\exists xG(x)$。故对任意$x\in D$，$G(x)$都是假命题，从而$\neg G(x)$都是真命题，故I满足$\forall x(\neg G(x))$。

若I弄假$\neg(\exists xG(x))$，则I满足$\exists xG(x)$。故有$x_0\in D$，使得$G(x_0)$是真命题。从而$\neg G(x_0)$是假命题，故I弄假$\forall x(\neg G(x))$。

其它等式同理可证。

引理2 设G,H是两个公式，其中自由变量有且只有一个x，分别记以$G(x)$，$H(x)$，于是有：

1) $\forall xG(x)\wedge\forall xH(x)=\forall x(G(x)\wedge H(x))$

2) $\forall xG(x)\vee\exists xH(x)=\exists x(G(x)\vee H(x))$

3) $\forall xG(x)\vee\forall xH(x)=\forall x\forall y(G(x)\vee H(y))$

4) $\exists xG(x)\wedge\exists xH(x)=\exists x\exists y(G(x)\vee H(y))$

证明：用类似于证明引理1的方法，可证明此引理的1)，2)。

3) $\forall xG(x)\vee\forall xH(x)$

$=\forall xG(x)\vee\forall yH(y)$ 改名规则

$=\forall x(G(x)\vee\forall yH(y))$ 引理1

$=\forall x\forall y(G(x)\vee H(y))$ 引理1

同理可证4)。

定理1 对任意公式G，都存在与其等价的前束范式。

证明：通过如下算法，可将公式G化成等价的前束范式。

1. 使用基本等价式

$(K\leftrightarrow H)=(K\rightarrow H)\wedge(H\rightarrow K)$

$(K\rightarrow H)=\neg K\vee H$

可将公式G中的$\leftrightarrow$和$\rightarrow$删除。

2. 使用$\neg(\neg H)=H$，De Morgan律，引理1，可将公式中所有否定号$\neg$放在原子之前。

3. 如果必要的话，则将约束变量改名。

4. 使用引理1，2将所有量词都提到公式的最左边。

于是，将公式G在等价意义下化成了一个前束范式。

例如， $\forall x\forall y(\exists z(P(x,z)\wedge P(y,z))\rightarrow\exists uQ(x,y,u))$

$=\forall x\forall y(\neg(\exists z(P(x,z)\wedge P(y,z)))\vee\exists uQ(x,y,u))$

$=\forall x\forall y(\forall z(\neg P(x,z)\vee\neg P(y,z))\vee\exists uQ(x,y,u))$

$=\forall x\forall y\forall z(\neg P(x,z)\vee\neg P(y,z)\vee\exists uQ(x,y,u))$

$=\forall x\forall y\forall z\exists u(\neg P(x,z)\vee\neg P(y,z)\vee Q(x,y,u))$

下面我们将介绍另一种比前束范式还要好的标准形式，即在首标中没有存在量词出现的特殊的前束范式。通常称之为Skolem范式。

定义 设 G 是一个公式，$Q_1x_1\cdots Q_nx_nM$ 是与 G 等价的前束范式，其中 M 为合取范式形式。若 Q_r 是存在量词，并且它左边没有全称量词，则取异于出现在 M 中所有常量符号的常量符号 c，并用 c 代替 M 中所有的 x_r，然后在首标中删除 Q_rx_r。

若 $Q_{s1},\cdots,Q_{sm}$ 是所有出现在 Q_rx_r 左边的全称量词（$m\geq 1, 1\leq s1<s2<\cdots<sm<r$），则取异于出现在 M 中所有函数符号的 m 元函数符号 $f(x_{s1},\cdots,x_{sm})$，用 $f(x_{s1},\cdots,x_{sm})$ 代替出现在 M 中的所有 x_r，然后在首标中删除 Q_rx_r。

对首标中的所有存在量词做上述处理后，得到一个在首标中没有存在量词的前束范式，这个前束范式就称为公式 G 的 Skolem 范式。其中用来代替 x_r 的那些常量符号和函数符号称为公式 G 的 Skolem 函数。

例如，$G=\exists x\forall y\forall z\exists u\forall v\exists wP(x,y,z,u,v,w)$

用 a 代替 x，

用 $f(y,z)$ 代替 u，

用 $g(y,z,v)$ 代替 w，

得公式 G 的 Skolem 范式：

$\forall y\forall z\forall vP(a,y,z,f(y,z),v,g(y,z,v))$。

下面我们来讨论公式 G 与它的 Skolem 范式 S 之间的关系。

1. G 与 S 的可满足性是等价的。

证明：设 G 是前束范式：

$$G = Q_1x_1\cdots Q_nx_nM(x_1,\cdots,x_n)$$

设 Q_r 是从左往右看第一个存在量词。令

$$G_1 = \forall x_1\cdots\forall x_{r-1}Q_{r+1}x_{r+1}\cdots Q_nx_nM(x_1,\cdots,x_{r-1},f(x_1,\cdots,x_{r-1}),x_{r+1},\cdots,x_n)$$

其中 $f(x_1,\cdots,x_{r-1})$ 是代替 x_r 的 Skolem 函数。

下面证明 1）满足 G_1 的解释满足 G，2）满足 G 的解释，适当扩充后可满足 G_1。

设个体域为 D，取一个满足 G_1 的解释 I，于是，对每一组 $(x_1'\cdots,x_{r-1}')\in D^{r-1}$，都有 $f(x_1',\cdots,x_{r-1}')\in D$，使得

$$Q_{r+1}x_{r+1}\cdots Q_nx_nM(x_1',\cdots,x_{r-1}',f(x_1',\cdots,x_{r-1}'),x_{r+1},\cdots,x_n)$$

在 I 下取 1 值。所以 $\forall x_1\cdots\forall x_{r-1}\exists x_rQ_{r+1}x_{r+1}\cdots Q_nx_nM(x_1,\cdots,x_n)$ 为真，即 I 满足 G。

反之，取一个满足 G 的解释 I。于是，对每一组 $(x_1'\cdots,x_{r-1}')\in D^{r-1}$，都存在 $x_r'\in D$，使得

$$Q_{r+1}x_{r-1}\cdots Q_nx_nM(x_1',\cdots,x_{r-1}',x_r',x_{r+1},\cdots,x_n)$$

在 I 下取 1 值。现在 I 还不是 G_1 的解释，因为有函数没有指定，扩充 I 为 I'，使其包含对函数符号 $f(x_1,\cdots,x_{r-1})$ 的如下指定：

$f(x_1',\cdots,x_{r-1}')=x_r'$，对每一组 $(x_1',\cdots,x_{r-1}')(D_{r-1}$。于是 I' 满足 G_1。

同理，对 G_1 往右找下一个存在量词，用 Skolem 函数代替得 G_2，则 G_1 与 G_2 的可满足性是等价的。依此类推，可知 G 与 S 的可满足性是等价的。

例如，设 $G=\forall x\exists yP(x,y)$，则 G 的 Skolem 范式为 $S=\forall xP(x,f(x))$

设 $D=\{1,2\}$

取满足 S 的解释 I 如下：

$f(1)$	$f(2)$	$P(1,1)$	$P(1,2)$	$P(2,1)$	$P(2,2)$
2	1	任意	1	1	任意

则对 I 不看对函数的解释，也是 G 的解释，且满足 G。

反之，取满足 G 的解释 I 如下：

$P(1,1)$	$P(1,2)$	$P(2,1)$	$P(2,2)$
1	任意	1	任意

现在 I 还不是 S 的解释，因为有函数没有指定，扩充 I 为 I'，使其包括对函数的指定

$f(1)$	$f(2)$
1	1

则 I' 满足 S。

2. G 与 S 不等价

由 1 可知，满足 G 的解释 I，不一定满足 S，因为在扩充时，可随意指定 Skolem 函数的值。例如，$G=\exists xP(x)$，$S=P(a)$。令 G 和 S 的解释 I 如下：

$$D=\{2,3\},$$

a	$P(2)$	$P(3)$
2	0	1

则 I 满足 G，但 I 弄假 S。

3. G 与 S 的恒假性等价

定理 2　设 S 是公式 G 的 Skolem 范式，于是，公式 G 是恒假的充要条件是公式 S 是恒假的。

证明：若 G 恒假，而 S 可满足，由 1 知，G 是可满足的，矛盾。

若 S 恒假，而 G 可满足，由 1 知，S 是可满足的，矛盾。

故定理成立。

请读者考虑 G 与 S 的恒真性是否等价。

习　题

1. 试将下列公式化成等价的前束范式：

a) $\forall x(P(x)\rightarrow\exists yQ(x,y))$；

b) $\exists x((\neg\exists yP(x,y))\rightarrow(\exists zQ(z)\rightarrow R(x)))$；

c) $\forall x\forall y(\exists zP(x,y,z)\wedge(\exists uQ(x,u)\rightarrow\exists vQ(y,v)))$。

2. 找出下面公式的 Skolem 范式：

a) $\neg(\forall xP(x)\rightarrow\exists y\forall zQ(y,z))$；

b) $\forall x(\neg E(x,0)\rightarrow(\exists y(E(y,g(x))\wedge\forall z(E(z,g(x))\rightarrow E(y,z)))))$。

3. 假设 $\exists x\forall yM(x,y)$ 是公式 G 的前束范式，其中 $M(x,y)$ 是仅仅包含变量 x,y 的母式。设 f 是不出现在 $M(x,y)$ 中的函数符号，证明：G 是恒真的当且仅当 $\exists xM(x,f(x))$ 是恒真的。

§4　例

在本节中，将给出一些例子，说明日常生活中的命题和数学中的命题，如何写成一阶逻辑中的符号公式。当然，由于日常生活中的一句话往往是概念模糊的，因此，描述成公式的方式也不是唯一的。例如："不管黑猫白猫，抓住老鼠就是好猫"这句话，所谓不管黑猫白猫，是只限制为黑猫白猫？还是包含别色的猫？所谓抓住老鼠，是指抓住所有老鼠？还是指至少抓住一只就可以？因此，我们在描述这些命题时，总是将这些模糊概念做某种确切理解。

例 1　每一个人都爱他自己的孩子。

令　$P(x)$：x 是人；

$C(x)$：x 是孩子；

$I(x,y)$：x 属于 y；

$L(x,y)$：x 爱 y，

此命题在一阶逻辑中表示为：

$$\forall x \forall y(P(y) \land C(x) \land I(x,y) \to L(y,x))$$

例 2 假设有一个人被每一个喜欢某些人的人所喜欢，又假设没有不喜欢人的人。证明：有一个人被所有的人喜欢。

令 $L(x,y)$：x 喜欢 y，

前提的描写：

P_1：$\exists y \forall x(\exists z L(x,z) \to L(x,y))$；

P_2：$\neg\exists x \forall y(\neg L(x,y))$，

结论的描写：

C：$\exists x \forall y L(y,x)$，

于是，要去证明：$(P_1 \land P_2) \to C$ 是恒真公式。

例 3 每一个人的外祖父都是他母亲的父亲。

令 $P(x)$：x 是人；

$O(x,y)$：x 是 y 的外祖父；

$F(x,y)$：x 是 y 的父亲；

$M(x,y)$：x 是 y 的母亲，

于是命题可表为：

$$\forall x \forall y(P(y) \land O(x,y) \to \exists z(F(x,z) \land M(z,y)))$$

例 4 不管黑猫白猫，抓住老鼠就是好猫

令 $C(x)$：x 是猫；

$W(x)$：x 是白的；

$B(x)$：x 是黑的；

$G(x)$：x 是好的；

$M(x)$：x 是老鼠；

$K(x,y)$：x 抓住 y，

于是，命题可表示为：

$$\forall x \forall y(C(x) \land M(y) \land (B(x) \lor W(x)) \land K(x,y) \to G(x))$$

例 5 有些病人相信所有的医生，但是病人都不相信一个骗子。证明：医生都不是骗子。

令 $P(x)$：x 是病人；

$D(x)$：x 是医生；

$Q(x)$：x 是骗子；

$L(x,y)$：x 相信 y，

前提的描写：

G_1：$\exists x(P(x) \land \forall y(D(y) \to L(x,y)))$；

G_2：$\forall x \forall y(P(x) \land Q(y) \to \neg L(x,y))$，

结论的描写：

C：$\forall x(D(x) \to \neg Q(x))$，

于是，要去证明：$(G_1 \wedge G_2) \rightarrow C$ 是恒真公式

下面我们就证明这件事。

对任意解释 I（其中非空区域集合为 D），

若 I 弄假 $G_1 \wedge G_2$，则公式 $(G_1 \wedge G_2) \rightarrow C$ 为真。

若 I 满足 $G_1 \wedge G_2$，那么，

因为 G_1 在 I 下为真，所以存在 $e \in D$，使

$$P(e) \wedge \forall y(D(y) \rightarrow L(e,y)) \tag{1}$$

在 I 下为真。

因为 G_2 在 I 下为真，所以对任意 $x \in D$、$y \in D$，都有 $P(x) \wedge Q(y) \rightarrow \neg L(x,y)$ 是真的。特别，

$$P(e) \wedge Q(y) \rightarrow \neg L(e,y) \tag{2}$$

是真的。

由(1)，(2)式知，对任意 $y \in D$，都有

$$D(y) \rightarrow L(e,y) \tag{3}$$

$$Q(y) \rightarrow \neg L(e,y) \tag{4}$$

是真的。亦即：对任意 $y_0 \in D$，若 $D(y_0)$ 在 I 下为真，则由(3)知，$L(e,y_0)$ 在 I 下为真，由(4)知，$Q(y_0)$ 在 I 下为假，故 $\neg Q(y_0)$ 在 I 下为真。所以，对任意 $y_0 \in D$，命题 $(D(y_0) \rightarrow \neg Q(y_0))$ 是真的。故 I 满足 $\forall x(D(x) \rightarrow \neg Q(x))$。即 I 满足 C。所以，$(G_1 \wedge G_2) \rightarrow C$ 是恒真的。

例 6　每一个有理数都是实数；

某些实数是有理数；

不是每一个实数都是有理数。

令　$P(x)$：x 是有理数；

$Q(x)$：x 是实数。

上述三个命题符号化如下：

$$\forall x(P(x) \rightarrow Q(x));$$

$$\exists x(Q(x) \wedge P(x));$$

$$\neg(\forall x(Q(x) \rightarrow P(x)))$$

例 7　对平面上任意两点，有且仅有一条直线通过这两点。

令　$P(x)$：x 是一个点；

$L(x)$：x 是一条直线；

$R(x,y,z)$：z 通过 x、y；

$E(x,y)$：x 等于 y，

命题符号化如下：

$$\forall x \forall y(P(x) \wedge P(y) \rightarrow \exists z(L(z) \wedge R(x,y,z) \wedge \forall u(L(u) \wedge R(x,y,u) \rightarrow E(u,z))))。$$

例 8　在实数集中，任给一正实数，都存在大于该实数的实数。

令　$R(x)$：x 是实数；

$G(x,y)$：x 大于 y。

命题可符号化如下：

$$\forall x(R(x) \wedge G(x,0) \rightarrow \exists y(R(y) \wedge G(y,x)))。$$

例 9　设 $f_1(x)$，…$f_n(x)$，…是函数序列，$f(x)$ 是一个函数。"对任给 $\varepsilon > 0$，$x_0 \in (a,b)$，都存

在 N，使当 $n>N$ 时，有

$$|f(x_0)-f_n(x_0)|<\varepsilon$$

则称函数序列 $\{f_n(x)\}$ 在 (a,b) 区间内收敛于 $f(x)$。

令 $G(x,y)$：x 大于 y；

$B(x)$：x 属于 (a,b) 区间；

$s(x,n)$：$f(x)$ 与 $f_n(x)$ 之差的绝对值，

于是，函数序列收敛的概念可符号化如下：

$$\forall x\forall \varepsilon(G(\varepsilon,0)\land B(x)\to\exists N\forall n(G(n,N)\to G(\varepsilon,s(x,n))))。$$

例 10 设 $f_1(x),\cdots,f_n(x),\cdots$ 是函数序列，$f(x)$ 是一个函数。“对任给 $\varepsilon>0$，都存在 N，使当 $n>N$ 时，对所有 $x\in(a,b)$，都有

$$|f(x)-f_n(x)|<\varepsilon$$

则称函数序列 $\{f_n(x)\}$ 在 (a,b) 区间内一致收敛于 $f(x)$。

令 $G(x,y)$：x 大于 y；

$B(x)$：x 属于 (a,b) 区间；

$s(x,n)$：$f(x)$ 与 $f_n(x)$ 之差的绝对值，

于是，函数序列一致收敛的概念可符号化如下：

$$\forall \varepsilon(G(\varepsilon,0)\to\exists N\forall n(G(n,N)\to\forall x(B(x)\to G(\varepsilon,s(x,n)))))。$$

习　　题

1. 将下面的命题符号化，并证明之。
   a) 已知每一个大学生都是诚实的，而约翰是不诚实的，证明约翰不是大学生。
   b) 已知每一个运动员都是强壮的，而每一个既强壮又聪明的人在他所从事的事业中都将获得成功，彼得是运动员并且是聪明的，证明彼得在他的事业中将会成功。
   c) 已知海关人员检查每一个进入本国的不重要人物，某些走私者进入该国时仅仅被走私者所检查，没有一个走私者是重要人物，证明海关人员中的某些人是走私者。
2. 将下面的命题符号化：
   a) 函数序列 $\{f_n(x)\}$ 在 (a,b) 区间内不收敛于函数 $f(x)$。
   b) 函数序列 $\{f_n(x)\}$ 在 (a,b) 区间内不一致收敛于函数 $f(x)$。

第四章　图

§1　图

现实世界中，有许多事情可以用由点和线组成的图形来描述。例如，国家用点来表示，有外交关系的两个国家就用线来连接代表这两个国家的点，于是，世界各国之间的外交关系就被一个由点和线组成的图形描述出来了。又如，城市之间的交通联系或通讯联系，也可以被一个由点和线组成的图形描述。在这些图形中，我们感兴趣的是哪些点之间有线连接，而不关心这些点是什么，以及这些点之间的连接方式如何。这种数学抽象就是图的概念。

定义　$G=(P,L)$称为图，如果 P 是非空的点的集合，L 是连接某些不同点对的边集合，并且任意一对不同点之间最多有一条边，当 P 为有限集时，G 称为有限图。

没有任何边的图称为空图，只有一个点的图称为平凡图。任意两点之间都有边的图称为完全图。

设 $G=(P,L)$是一个图，今后，我们用 $P(G)$表示 G 的点集，用 $L(G)$表示 G 的边集。设 $l\in L(G)$，并假设 l 是连接 G 中点 u、点 v 的边，则称 u、v 是 l 的端点，并称 u 与 v 相邻。有时，在不致引起混乱的情况下，将 l 记为 uv。

注意　1. 在研究图时，重点放在点及连接点的边上，点的位置及边的形状无关紧要，一个图可能因点的位置不同或边的形状不同而表示成外部形状截然不同的图，如：



我们把上面这两个图看成是同样的图，有的书称为同构。

2. 不允许出现点到其自身的边。

3. 不同点之间不允许有两条及两条以上的边。

(有些书把满足 2，3 的图称为简单图)

4. 不能用直观代替证明。

定义　设 G，H 是图，如果 $P(H)\subseteq P(G)$，$L(H)\subseteq L(G)$，则称 H 是 G 的子图，G 是 H 的母图；如果 H 是 G 的子图，并且 $P(H)=P(G)$，则 H 是 G 的支撑子图。

定义　设 G 是图，$v\in P(G)$，$L(G)$中以 v 为端点的边的条数称为点 v 的度，记为 $d_G(v)$。

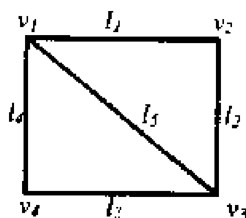
今后，为简便计，有时也将图 G 中的点 v、边 l，写成 $v\in G$，$l\in G$。

定义　设 $G=(P,L)$是有限图，集合 P 的元数为 m，集合 L 的元数为 n，不妨设 $P(G)=\{v_1,\cdots,v_m\}$，$L(G)=\{l_1,\cdots,l_n\}$。矩阵 $M(G)=[a_{ij}]$称为 G 的关联矩阵，其中

$$a_{ij}=\begin{cases}0, & \text{当 } v_i \text{ 不是 } l_j \text{ 的端点}\\ 1, & \text{当 } v_i \text{ 是 } l_j \text{ 的端点}\end{cases}$$

显然，$M(G)$是$m\times n$阶矩阵。

例如，下面的图及其关联矩阵为：



$$M(G)=\begin{bmatrix}1&0&0&1&1\\1&1&0&0&0\\0&1&1&0&1\\0&0&1&1&0\end{bmatrix}$$

关联矩阵的特点：

(1) $M(G)$中每一列恰有两个1，表示每一边有两个端点；

(2) 每一行1的个数为对应该行点的度。

一个图可以用其关联矩阵表示，也可用下面的所谓相邻矩阵$A(G)=[b_{ij}]$表示，其中

$$b_{ij}=\begin{cases}0, & \text{当 } v_i \text{ 与 } v_j \text{ 不相邻}\\1, & \text{当 } v_i \text{ 与 } v_j \text{ 相邻}\end{cases}$$

显然，$A(G)$是$m\times m$阶方阵。

例如，上图的相邻矩阵为：

$$A(G)=\begin{bmatrix}0&1&1&1\\1&0&1&0\\1&1&0&1\\1&0&1&0\end{bmatrix}$$

相邻矩阵的特点：

(1) 相邻矩阵是一对称矩阵；

(2) 每行(列)1的个数为该点的度。

定理1 是$G=(P,L)$是有限图，不妨设$L(G)$含有m个元素，于是

$$\sum_{v\in P(G)} d_G(v)=2m$$

证明：设$M(G)$是G的关联矩阵，因为G中某点v的度$d_G(v)$恰是$M(G)$中代表点v的那一行中1的个数，故

$$\sum_{v\in P(G)} d_G(v)=M(G)\text{ 中 1 的个数}$$

而$M(G)$中每列恰有两个1，$M(G)$共有m列，故$M(G)$中1的个数为$2m$。所以

$$\sum_{v\in P(G)} d_G(v)=2m$$

定理2 任意有限图中，奇数度点的个数是偶数。

证明：设S_1、S_2分别是图G中有奇数度的点，有偶数度的点的集合，由定理1知：

$$\sum_{v\in S_1} d_G(v)+\sum_{v\in S_2} d_G(v)$$

是偶数。因为$\sum_{v\in S_2} d_G(v)$是偶数，所以$\sum_{v\in S_1} d_G(v)$是偶数。即$|S_1|$个奇数的和为偶数，而只有偶数个奇数的和才能是偶数，故S_1的元数是偶数。

例如，在任意n个自然数中，与其中奇数个数互质的数的个数一定是偶数。

让n个数作为图中的n个点，若两个数互质则在对应的两个点之间连一条边，由定理2知结论显然成立。

定义　设 $G=(P,L)$ 是图，v,v' 是 G 中两点。由 G 中点组成的序列 $(v_0,\cdots,v_n)$ 称为从 v 到 v' 的长度为 n 的**路**，如果

1) $v_0=v, v_n=v'$；

2) v_i 与 v_{i+1} 相邻，$0\leq i<n$。

定义　设 $G=(P,L)$ 是图，$(v_0,\cdots,v_n)$ 是 G 中从 v_0 到 v_n 的路。称此路为**简单路**，如果

1) $v_0,\cdots,v_{n-1}$ 互不相同；

2) $v_1,\cdots,v_n$ 互不相同。

显然，一条简单路 $(v_0,\cdots,v_n)$，除 v_0 与 v_n 可以相同外，其它任何两点都不相同。

定义　设 $G=(P,L)$ 是图。G 中从点 v 到自身的其长度不小于 3 的简单路，称为**回路**。

设 $G=(P,L)$ 是图，G 中两点 u,v，如果从 u 到 v 有一条路，则称 u 与 v 是**相连的**。如果我们认为点 v 与自身是相连的，则显然 G 中两点之间的相连关系是一个等价关系。在此等价关系下，集合 $P(G)$ 必分成一些等价类，不妨设为 $S_1,\cdots,S_n,\cdots$。显然，每一个 S_i 和 G 中所有以 S_i 中的点为端点的边一起，组成 G 的一个子图 G_i。每个 G_i 称为 G 的一个**分支**。如果图 G 仅有一个分支，则称图 G 是**连通的**。对于图 G，我们用 $W(G)$ 记其分支数。

显然，一个图 G 是连通的，当且仅当 G 中任意两点都是相连的。

定义　设 $G=(P,L)$ 是有限图，如果对 $L(G)$ 中任一条边 l，都规定一个实数 $w(l)$ 附着其上，则称 G 为**权图**，称 $w(l)$ 为边 l 的**权**。规定 $w(uu)=0$（其中 $u\in P(G)$），$w(uv)=\infty$（其中 $uv\notin L(G)$）。

例如，一个描述各城市之间的铁路交通图，图中的每一边可以用这条边所表示的铁路长度为其权，于是这个铁路交通图就是权图。这个铁路交通图，也可以用每条边所代表的铁路修建费用为其权，那么这个铁路交通图又是一个权图。

可以想到，在一个权图 G 中，求出所带的权达到最小的那条路是有实际意义的，这就是图中求*最短路*问题。这条最短路所带的权称为*从 u 到 v 的距离*，记为 $d(u,v)$。

1959 年，Dijkstra 给出了一个在权图中求其任意两点间最短路的算法，该算法不是孤立地计算从 u_0 出发到 v 的最短路，而是统一考虑，利用该算法一次求出从 u_0 出发到所有其余顶点的最短路，该算法始终用一个点到一个点集的最短路代替点到点之间的最短路，减少了需要考虑的路的条数。下面我们介绍点到点集的最短路及距离的概念：

设 $G=(P,L)$ 是一个图，S 是由 G 中某些顶点做成的集合，$\bar{S}=P-S$，u_0 是 S 中一个点，*从 u_0 到 $\bar{S}$ 的最短路*是从 u_0 开始到 $\bar{S}$ 中点的路且该路的权和是最小的，这个最小的权和称为 *u_0 到 $\bar{S}$ 的距离*，记为 $d(u_0,\bar{S})$。

Dijkstra 算法　设 $G=(P,L)$ 是权图，$P=\{u_0,\cdots,u_n\}$

1) 令 $S_0=\{u_0\}$，$\bar{S}_0=\{u_1,\cdots,u_n\}$

计算 $d(u_0,\bar{S}_0)=\min\limits_{\substack{u\in S_0\\ v\in \bar{S}_0}}\{d(u_0,u)+w(uv)\}$

$=\min\limits_{v\in\bar{S}_0}\{w(u_0v)\}$

即：列举所有的 $w(u_0v)$，取其中最小者，得 $d(u_0,\bar{S}_0)$

不妨设实现 $d(u_0,\bar{S}_0)$ 的路是 $l_1=(u_0,u_1)$，$|l_1|=d(u_0,\bar{S}_0)$

l_1 就是 u_0 到 u_1 的最短路，$d(u_0,u_1)=d(u_0,\bar{S}_0)$。

2) 令 $S_1=\{u_0,u_1\}$，$\bar{S}_1=P-S_1=\{u_2,\cdots,u_n\}$

计算 $d(u_0,\overline{S}_1)=\min\limits_{\substack{u\in S_1\\v\in\overline{S}_1}}\{d(u_0,u)+w(uv)\}$

即：列举 $w(u_0u_2),\cdots,w(u_0u_n)$

$|l_1|+w(u_1u_2),\cdots,|l_1|+w(u_1u_n)$

取其中最小者，得 $d(u_0,\overline{S}_1)$，设实现此距离的路是 $l_2=(u_0,\cdots,u_2)$

l_2 就是 u_0 到 u_2 的最短路，$d(u_0,u_2)=d(u_0,\overline{S}_1)=|l_2|$

3) 设我们已求出 u_0 到 $u_1,\cdots,u_k$ 的最短路，设为 $l_1,\cdots,l_k$，

则取 $S_k=\{u_0,\cdots,u_k\}$，$\overline{S}_k=\{u_{k+1},\cdots,u_n\}$

计算 $d(u_0,\overline{S}_k)=\min\limits_{\substack{u\in S_k\\v\in\overline{S}_k}}\{d(u_0,u)+w(uv)\}$

即：列举 $w(u_0u_{k+1}),\cdots,w(u_0u_n)$

$|l_1|+w(u_1u_{k+1}),\cdots,|l_1|+w(u_1u_n)$

.

.

.

$|l_k|+w(u_ku_{k+1}),\cdots,|l_k|+w(u_ku_n)$

取其中最小者，为 $d(u_0,\overline{S}_k)$，设实现 $d(u_0,\overline{S}_k)$的路为 $l_{k+1}=(u_0,\cdots,u_{k+1})$

则 l_{k+1}是 u_0 到 u_{k+1}的最短路，$d(u_0,u_{k+1})=d(u_0,\overline{S}_k)=|l_{k+1}|$。

下面我们来证明 Dijkstra 算法的正确性：

已知 $d(u_0,\overline{S}_k)=\min\limits_{\substack{u\in S_k\\v\in\overline{S}_k}}\{d(u_0,u)+w(uv)\}$

设实现此距离的路为 l_{k+1}，此路在 $\overline{S}_k$ 中的终点为 u_{k+1}，

往证：$d(u_0,u_{k+1})=d(u_0,\overline{S}_k)$，$u_0$ 到 u_{k+1}的最短路就是 l_{k+1}，

证明：对 S_k 中的元数个数使用数学归纳法。

(1) 当 $|S_k|=1$ 时，$S_0=\{u_0\}$

此时 $d(u_0,\overline{S}_0)=\min\limits_{\substack{u\in S_0\\v\in\overline{S}_0}}\{d(u_0,u)+w(uv)\}$

设 $l_1=(u_0,u_1)$是实现 $d(u_0,\overline{S}_0)$的最短路，显然 $d(u_0,u_1)=d(u_0,\overline{S}_0)$

l_1 是 u_0 到 u_1 的最短路。

(2) 假设我们已经求出了 $d(u_0,u_1),\cdots,d(u_0,u_k)$和实现上述距离的最短路 $l_1,\cdots,l_k$，此时

$$S_k=\{u_0,u_1,\cdots,u_k\},\overline{S}_k=\{u_{k+1},\cdots,u_n\}$$

$$d(u_0,\overline{S}_k)=\min_{\substack{u\in S_k\\v\in\overline{S}_k}}\{d(u_0,u)+w(uv)\} \quad (*)$$

设实现 $d(u_0,\overline{S}_k)$的路 l_{k+1}在 $\overline{S}_k$ 中的终点为 u_{k+1}，往证 $d(u_0,u_{k+1})=d(u_0,\overline{S}_k)$。

l_{k+1}是 u_0 到 u_{k+1}的最短路，即证明对任意从 u_0 到 u_{k+1}的路 $l=(u_0,v_1,\cdots,v_r,u_{k+1})$，有 $|l|\geqslant|l_{k+1}|$。

首先，对任意 $v\in\overline{S}_k$，有 $w(u_0v)\geqslant|l_{k+1}|$　　(在(*)式中把 u 取成 u_0)

以下分三种情况讨论

A. l 第一步就跨入 $\overline{S}_k$，显然 $|l|\geq w(u_0v_1)\geq|l_{k+1}|$

B. 若 l 是在 S_k 中走，最后一步到达 u_{k+1}，由 l_{k+1}的取法知 $|l|\geq|l_{k+1}|$

C. l 先在 S_k 中走，中间进入 $\overline{S}_k$，最后到达 u_{k+1}，

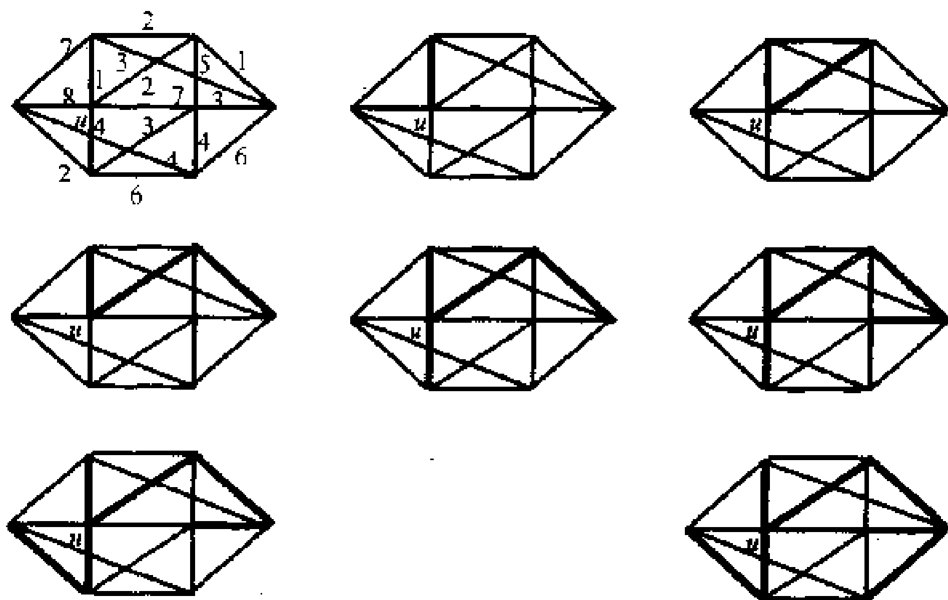
不妨设在 v_i 处跨入 $\overline{S}_k$，即 $v_i \in S_k$，$i \leq r$，则

$$|l_{k+1}| \leq |(u_0, v_1, \cdots, v_i)| \leq |(u_0, v_1, \cdots, v_r, u_{k+1})|$$

综上知，l_{k+1}是从 u_0 到 u_{k+1}的最短路。

此算法不但给出求两点距离的方法，而且一次性能求出一个点到其它所有点的距离。

例如，在下面权图中，从点 u 到其余 7 个点的最短路我们用粗线给出。



习　　题

1. 若 $G=(P,L)$是有限图，设 $P(G)$、$L(G)$的元数分别为 m，n。证明：$n \leq C_m^2$，其中 C_m^2 表示 m 中取 2 的组合数。

2. 设 G 是有限图，M，A 分别是 G 的关联矩阵和相邻矩阵，证明：MM' 和 A^2 的对角线上的元素是 G 中所有点的度。

3. 设 G 是有限图，$P(G)$，$L(G)$的元数分别为 m，n。δ，Δ 分别是 G 中点的最小度和最大度。证明：$\delta \leq 2n/m \leq \Delta$。

4. 设 G 是图，δ 是 G 中点的最小度。如果 $k \leq \delta$，则 G 中有一条长度为 k 的简单路。

5. 设 $G=(P,L)$是有限图，$P(G)$，$L(G)$的元数分别为 m，n。证明：如果 $n > C_{m-1}^2$，则 G 是连通的。

6. 证明：连通图中任意两条最长的简单路必有公共点。

7. 一公司在六个城市 c_1，c_2，$\cdots$，c_6 中的每一个都有分公司。从 c_i 到 c_j 的班机旅费由下列矩阵中的第 i 行第 j 列元素给出（∞表示没有直接班机）：

$$\begin{bmatrix} 0 & 50 & \infty & 40 & 25 & 10 \\ 50 & 0 & 15 & 20 & \infty & 25 \\ \infty & 15 & 0 & 10 & 20 & \infty \\ 40 & 20 & 10 & 0 & 10 & 25 \\ 25 & \infty & 20 & 10 & 0 & 55 \\ 10 & 25 & \infty & 25 & 55 & 0 \end{bmatrix}$$

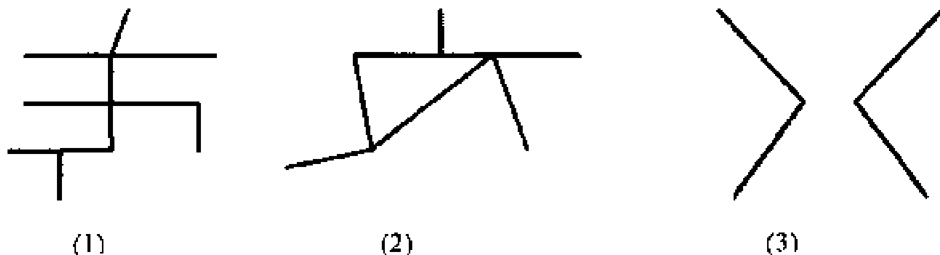
公司所关心的是计算两城市间的最便宜路线的表格。请准备一张这样的表格。

§2 树

树是计算机科学中一种经常使用的数据结构，本节我们简要介绍树的一些性质和算法。

定义 设$G=(P,L)$是图，如果G是连通的，并且无回路，则称G是树。

例如，图4.2.1中(1)是树，(2)，(3)不是树。



(1) (2) (3)

图4.2.1

把树的图形画出来，很象自然界中的树，故取名为树，而且关于树的其它术语，也取名于自然界中树的有关术语。

为了介绍树的性质，我们先证明下述重要引理。

引理1 设G是至少有一条边的有限图，且无回路，则G至少有一个点只相邻于另一点。

证明：因为G至少有一条边，所以G有一点v_1，且v_1有相邻点v_2。

若v_2即为所求，则引理得证。

否则，令v_3为v_2的相邻点，以此类推，亦即，对$k\geq 2$，或者v_k只与v_{k-1}相邻，从而v_k即为所求；或者v_k又相邻于$v_{k+1}\neq v_{k-1}$。于是得$v_1,v_2,\cdots,v_{k-1},v_k,v_{k+1}$，因为$G$无回路，故这一串点不能有重复，又因为$G$有限，故上述过程必在有限步内停止，故引理得证。

定理1 如果G是图，则下列诸命题等价：

(1) G是树；

(2) G连通并且删去G的任意一边，所得之图都不连通；

(3) 对G中任意两点$v,v'(v\neq v')$，恰有一条从v到v'的简单路；

如果G是有限图，设$P(G)$元数为n，则下列命题也与上面命题等价：

(4) G不含回路，并且G有$(n-1)$条边；

(5) G连通，并且G有$(n-1)$条边。

证明 (1)⇒(2)

设G是树，证明删除一边所得图不再连通。

采用反证法，设在G中删去边uv，所得图G'仍是连通的，于是G'的点u和v之间有路(u，

$v_1,\cdots,v_r,v)$，不妨假定$(u,v_1,\cdots,v_r,v)$是G'中从u到v的长度最短的路，$(r\geq 1)$，于是$(u,v_1,\cdots,v_r,v)$是G'中的简单路，因此，$(u,v_1,\cdots,v_r,v,u)$是G中回路，此与G是树矛盾。

(2)⇒(3)

因为G连通，所以对于v,v'，有从v到v'的路，取其中最短者，得从v到v'的简单路，若有两条这样的路，设为$(v,v_1,\cdots,v_n,v_{n+1})$，$(v,v_1',\cdots,v_m',v_{m+1}')$，其中$v_{n+1}=v_{m+1}'=v'$，从左向右看可找到最小的$k$，使得$v_k\neq v_k'$，于是，从$G$删去边$v_{k-1}v_k$，从$v_{k-1}$到$v_k$还有路$(v_{k-1},v_k',\cdots,v_{m+1}',v_n,v_{n-1},\cdots,v_k)$，故$G$删去边$v_{k-1}v_k$后，所得之图仍连通，矛盾。

(3)⇒(1)

由已知条件知，G是连通的，若G有回路$(v,v_1,\cdots,v_k,\cdots,v)$，则从$v$到$v_1$将有两条简单路：$(v,v_1)$和$(v,\cdots,v_k,\cdots,v_1)$，矛盾，故$G$中无回路，所以，$G$是树。

(1)⇒(4)

因为G是树，所以G中无回路，往证：G有$(n-1)$条边。

对n用归纳法。

$n=1$时，命题显然成立。

假设$n-1$时命题成立。

设G有n个点，由引理1知，G有点v_n，且v_n恰有一个相邻点v_{n-1}，删去v_n和v_nv_{n-1}得图G'。因为G无回路，所以G'无回路，因为G连通，所以G中任意两点间有路连接，因为v_n恰有一相邻点v_{n-1}，故点v_n只能出现在G中任意一条路的两端，而不能出现在中间，所以边v_nv_{n-1}只能出现在任意一条路的两端，所以删去点v_n和边v_nv_{n-1}，剩下的图中任意两点间仍有路，故G'连通。

因此，G'是树，由归纳假设，G'有$(n-1)-1$条边，故G有$(n-1)-1+1=n-1$条边。

(4)⇒(5)

已知G中无回路，有n个点，$(n-1)$条边，往证G连通，对n用归纳法。

$n=2$时，命题显然成立。

假设$n-1$时命题成立。

设G有n个点，由引理1知，G中有点v_n，v_n恰有一相邻点v_{n-1}。删去点v_n和边v_nv_{n-1}，得图G'。

显然，G'中仍无回路，但G'有$(n-1)$个点，由归纳假设，G'连通，因此，将点v_n和边v_nv_{n-1}添入G'，得G，G仍连通。

(5)⇒(1)

设G有n个点，$(n-1)$条边，并且连通，往证：G是树，显然，只须证G无回路即可。

若不然，设G有一条回路，则删去回路中任一条边，所得之图仍连通。对G中每一条回路，都用此法删去一边，最后得一个无回路但仍然连通的图G'，所以G'是树，而G'是由G删去$k(k>0)$条边所得，故G'仍有n个点，所以由(1)⇒(4)知，G'有$(n-1)$条边，但是G'有$(n-1-k)$条边，而$n-1>n-1-k$(因为$k>0$)，矛盾。

推论1　任一有限连通图必有一支撑子图是树。今后，把此支撑子图称为母图的支撑树。

推论2　若G'是有限图G的支撑树，vv'为G中一边，且vv'不在G'中，则G'添上边vv'后就有回路。

使用定理1不难证明上述两推论，故证明从略。

根树是计算机科学中经常使用的概念，我们从树的概念出发，对根树给出递归定义如下：

(1) 设 T 是树，其点集为 V，点集 V 中有一个特殊点 v_1，称为树的根。只由一个点构成的树是根树。

(2) 从 T 中删除 v_1 以及以 v_1 为端点的边后，所得图可分成 r 个分枝 $T_1,\cdots,T_i,\cdots,T_r$，每个 $T_i(i=1,\cdots,r)$ 也是一棵根树，T_i 称作 v_1 的子树。且每个 T_i 的根都在 T 中与 v_1 相邻，称为 v_1 的儿子。

次数≥2 的点又称为树的分枝点，次数为 1 的点称为树的叶。人们习惯上把树的根画在上方，叶画在下方。

例如，图 4.2.2 是一棵根树。

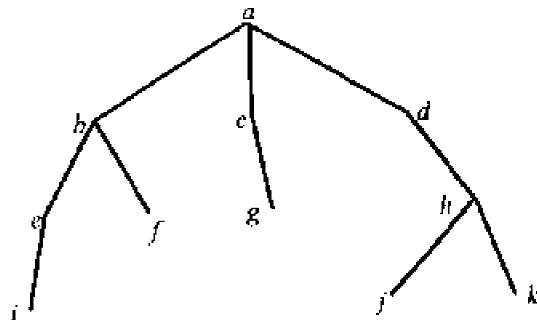


图 4.2.2

在本例的根树 T 中，a 是根，删去 a 以及以 a 为端点的边后，得三个分枝 T_1、T_2 和 T_3。每个分枝也是根树，其根分别为 b、c、d。

在此根树中，a、b、c、d、e、h 是分枝点。i、f、g、j、k 是叶。

人们在研究根树时，通常把树的根称为是子树的根的父亲，子树的根互相称为兄弟，而且都是它们父亲的儿子。根树的根是没有父亲的，叶是没有儿子的。

在图 4.2.2 中，a 有 3 个儿子 b，c，d。a 是 b，c，d 的父亲，b 是 e 和 f 的父亲，b 有两个儿子 e 和 f，等等。另外，b，c，d 是兄弟，e 和 f 也是兄弟。

定义 如果根树 T 的每个点 v 最多有两棵子树，则称 T 为二叉树。如果两棵子树全出现，则左边的一棵子树称为左子树，右边的一棵子树称为右子树；若仅出现一棵子树，则或者指定它为左子树，或者指定它为右子树。如果一棵根树的每个分枝点都有两棵子树，则称该树为完全二叉树。如图 4.2.3 是二叉树，也是完全二叉树：

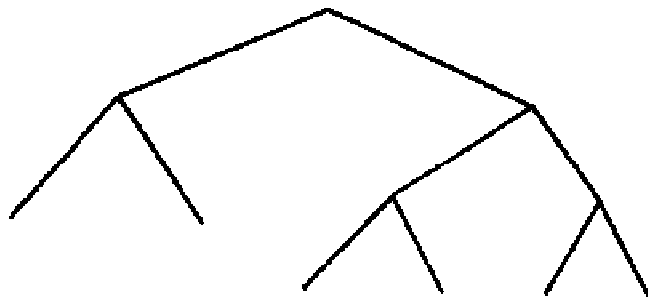


图 4.2.3

对于二叉树，一个十分重要的问题是找到一种方法访问树的所有点，并且每个点恰好被访

问一次，这就是二叉树的遍历问题。遍历二叉树的方法主要有三种。

(1)先根次序遍历法：{访问根；遍历左子树；遍历右子树}

(2)中根次序遍历法：{遍历左子树；访问根；遍历右子树}

(3)后根次序遍历法：{遍历左子树；遍历右子树；访问根}

例如，图 4.2.4 是一棵二叉树 T

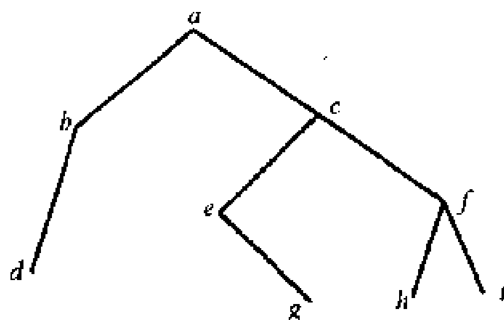


图 4.2.4

在先根次序下，T 上的点被访问的先后次序是

abdcegfhi

在中根次序下，T 上的点被访问的先后次序是

dbaegchfi

在后根次序下，T 上的点被访问的先后次序是

dbgehifca

二叉树在计算机科学中有着广泛的应用，进一步的知识请参阅数据结构。

下面我们来讨论一有实际意义的问题。

我们设想要建筑一个连接若干城市的铁路网。已知建造直接连接城市 v_i 与 v_j 的干线费用为 c_{ij}。试设计一个铁路网，以使建筑总费用达到最小。

将每个城市看作权图中一点，权图中任意两点 v_i，v_j，令 c_{ij}为边 v_iv_j 所带的权。显然，这个问题是在权图中求一个带权总数最小的连通支撑子图。又因为权代表费用，所以肯定它们是非负的，因此，这一带有最小权的支撑子图中没有回路，亦即，这个子图必是图 G 的支撑树。这个支撑树(带有最小权)称为权图 G 的最优树，上述建筑铁路的问题就是求一个权图中的最优树问题。

1956 年，Kruskal 给出了在权图中求最优树的算法。

Kruskal 算法：设 $G=(P,L)$是有限连通权图

A. 在 L 中选一个权具有最小值的边，记为 l_1，$w(l_1)\leqslant w(l)$，其中 $l\in L$，令 $T=\{l_1\}$。

B. 设 $T=\{l_1,\cdots,l_k\}$，在 $L-T$ 中选满足如下条件的边 l_{k+1}

1) 把 l_{k+1}并入 T 后不产生回路；

2) 在满足条件 1)的前提下,l_{k+1}的权最小。

C. 如果找不到满足条件 B 的边,则算法终止。

定理 2 设 $G=(P,L)$是连通权图,Kruskal 算法停止时得的图一定是 G 的最优支撑树。

证明:(1) 先证明 T 是支撑子图,即证明 $P(T)=P(G)$。

容易看出 $P(T)\subseteq P(G)$,往证 $P(G)\subseteq P(T)$。

用反证法,设 $x\in P(G)$,但 $x\notin P(T)$,任取 T 中点 y,因 G 是连通的,所以在 G 中有 x 到 y 的路 $l=(x,v_1,\cdots,v_r,y)$,则 xv_1 不是 T 中的边,把边 xv_1 加入 T 中不会产生回路,此与 T 终止在步骤 C 矛盾,所以,$P(G)=P(T)$。

(2) 证明 T 是一个树,只须证明 T 是连通的(无回路由算法保证)。

若 T 不连通,不妨假设 T 有两个分支 T_1 和 T_2,令 $x\in T_1,y\in T_2$,因 G 是连通的,所以有 G 中的路$(x,v_1,\cdots,v_i,v_{i+1})$,其中 $x=v_1,y=v_{r-1}$,因此,必有边 v_iv_{i+1},使 $v_i\in T_1,v_{i+1}\notin T_1$,那么,把 v_iv_{i+1}加到 T 中,不会产生回路,矛盾于算法停止,所以 T 是连通的。

(3) 由(1),(2)得,T 是支撑树,设 G 有 r 个顶点,T 有 $r-1$ 条边。

(4) 证明 T 是最优支撑树,我们证明可以通过以下不断交换边的办法,使 T 的所有边全在某一最优支撑树 T'中,则 $T=T'$(均有 $r-1$ 条边)。

设 T^* 是一棵最优支撑树,$T^*=\{l'_1,\cdots,l'_{r-1}\}$,$T=\{l_1,\cdots,l_{r-1}\}$,

若 $l_1\notin T^*$,在 T^* 中加入 l_1,则形成一含有 l_1 的回路,在此回路中删去一条非 l_1 的边,不妨设为 l'_1,得一图 T',令 $T'=\{l_1,l'_2,\cdots,l'_{r-1}\}$,则 T'是支撑树。

对任意 $l\in L(G)$,因为 $w(l_1)\leq w(l)$,所以 $w(l_1)\leq w(l'_1)$

而 $w(T')=T^*-w(l'_1)+w(l_1)$,所以 $w(T')\leqslant W(T^*)$,即 T'也是最优树。

一般地,设 $l_1,\cdots,l_k\in T^*,l_{k+1}\notin T^*,T=\{l_1,\cdots,l_k,l_{k+1},\cdots,l_{r-1}\},T*=\{l_1,\cdots,l_k,l'_{k+1},\cdots,l'_{r-1}\}$

因为 T^*是支撑树,$T^*\cup\{l_{k+1}\}$必然有回路 C,不妨设 l'_{k+1}是回路中一条边,$l'_{k+1}\notin T$,

令 $T'=\{l_1,\cdots,l_k,l_{k+1},l'_{k+2},\cdots,l'_{r-1}\}$,则 T'是支撑树,由 Kruskal 算法步骤 B,在算法实行中选了 l_{k+1}而没选 l'_{k+1},说明 $w(l_{k+1})\leqslant w(l'_{k+1})$

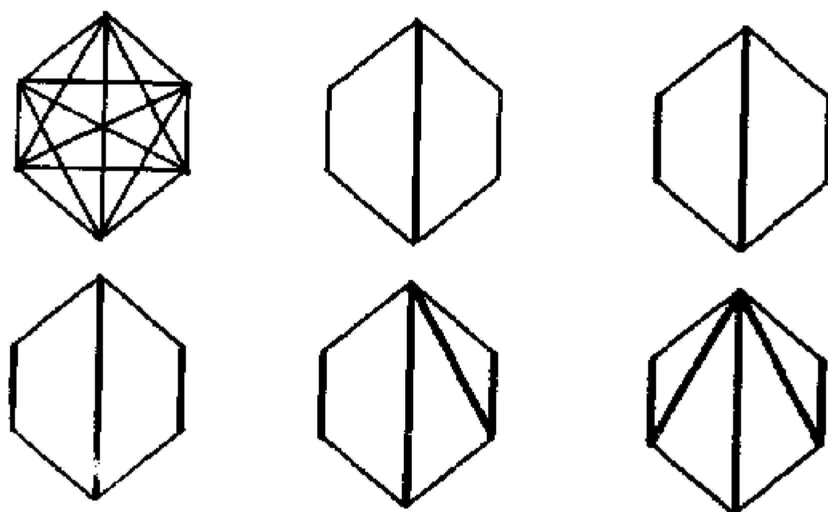
所以 $w(T')=w(T^*)-w(l'_{k+1})+w(l_{k+1})$,即 $w(T')\leqslant w(T^*)$

因为 T^*是最优树,所以 T'也是最优树,但 T'包括 $l_1,\cdots,l_{k+1}$,反复执行上述过程,最后可得一最优树包括了 T 的所有边,即 $T'=T$,所以 T 是最优树。

例如 世界上六大城市之间的航线距离表如下:(以 100 英里为 1 个单位)

	伦敦	墨西哥	纽约	巴黎	北京	东京
伦敦		55	34	2	50	59
墨西哥	55		20	57	77	70
纽约	34	20		36	68	67
巴黎	2	57	36		51	60
北京	50	77	68	51		13
东京	59	70	67	60	13	

用 Kruskal 算法,可求出连接此六城市的最短距离的航线网。



§3　有向图和有向树

本节讨论的有向图和有向树的概念，是为下一节讨论 Euler 路做准备的。因此，关于有向图和有向树的实际意义可以在下一节看出来。

定义　$G=(P,A)$称为有向图，如果 P 是非空点集，A 是从一点引到一点(不要求一定是另一点)的弧集。当 P 为有限集时，G 称为有限有向图。

若 e 是一条从点 v 到点 v' 的弧，则称 v 为 e 的起点，记为 $v=\text{init}(e)$；v' 为 e 的终点，记为 $v'=\text{fin}(e)$。

有向图中两点(可以是相同的)间的弧可以有无穷条。显然，有限有向图中的集合 A 未必是有限集。亦即，有限有向图中的弧可以有无穷多条。

有向图中点 v 的输出次数是集合$\{e|\text{init}(e)=v\}$的元数；点 v 的输入次数是集合$\{e|\text{fin}(e)=v\}$的元数；点 v 的度等于点 v 的输入次数加输出次数。

今后，为简便计，有时也将有向图 G 中的点 v，弧 e，写成 $v\in G$，$e\in G$。

定义　设 G，H 是有向图，如果 $P(H)\subseteq(G)$，$A(H)\subseteq A(G)$，则称 H 为 G 的有向子图(简称子图)。G 是 H 的母图。如果 H 是 G 的子图，并且 $P(H)=P(G)$，则称 H 是 G 的支撑子图。

定义　设 $G=(P,A)$是有向图，弧序列$(e_1,\cdots,e_n)$称为 G 的从 v 到 v' 其长度为 n 的有向路，如果

1) $e_i\in A(G)$，$i=1,\cdots,n$

2) $v=\text{init}(e_1)$，$v'=\text{fin}(e_n)$

3) $\text{fin}(e_k)=\text{init}(e_{k+1})$，$1\leq k\leq n-1$

在不能引起混乱的情况下，有时也将有向路$(e_1,\cdots,e_n)$写成$(v_1,\cdots,v_n,v_{n+1})$，其中 $v_i=\text{init}(e_i)$　$(i=1,\cdots,n)$，$v_{n+1}=\text{fin}(e_n)$。

定义　有向图 G 的有向路$(e_1,\cdots,e_n)$ 称为简单的，如果

1) $\text{init}(e_1),\cdots,\text{init}(e_n)$互不相同

2) $\text{fin}(e_1),\cdots,\text{fin}(e_n)$互不相同

定义 设$G=(P,A)$是有向图,$v\in P(G)$,从点v到自身的简单有向路(长度可以为1或2)称为有向回路。

例如,在图4.3.1中,弧e_1的起点是A,终点是B;点A的输出次数为1,输入次数为1;点B的输入,输出次数都为1,点C的输入次数是2,输出次数是1;(e_4),(e_7,e_1,e_2)都是从F到C的简单路。

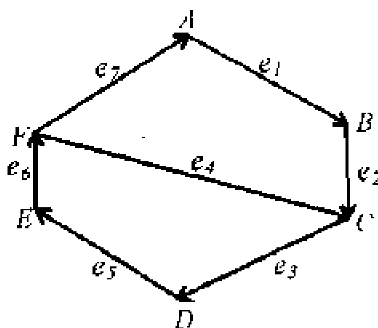


图4.3.1

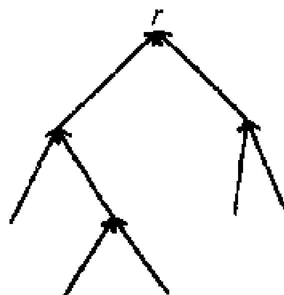


图4.3.2

定义 设$G=(P,A)$是有向图,对G中任意两点v,$v'(v\neq v')$,如果都有从v到v'的有向路,则称G是强连通的。

定义 设$G=(P,A)$是有向图,$r\in P(G)$。称r为G的根,如果对G中任意一点$v(v\neq r)$,都有从v到r的有向路。

显然,强连通图的每一点都是根,反之,每一点都是根的有向图也必是强连通的。

例如,上面的图4.3.1中每一点都是根,它是一个强连通的图;图4.3.2虽然不是强连通的,但有根r。

下面我们介绍有向图G的漠视图G_0:

(1) 删去G中自身到自身的弧;

(2) G中任意两点,若有弧,只保留一条;

(3) 删去弧的方向,即得G_0。

显然,若有向图G是强连通的,则G必有根;若有向图G有根,则漠视图G_0必连通。反之,不一定成立。亦即,若G_0连通,则G不一定有根;若有根,则G未必强连通。

定义 有向图G称为有向树(或有根树),如果G中有一点r,并且满足:

1) G中每一点$v(v\neq r)$都恰是一条弧的起点,

2) r不是任意一条弧的起点,

3) r是根。

从定义中我们可推出有向树有如下性质:

1) 每一点$v(v\neq r)$到r恰有一条有向路;

2) 没有有向回路;

3) 两点间最多有一条弧。

例如,图4.3.2就是一个有向树。

定理1(转化定理) 对有向树G,若无视各弧之方向,则得一树G_0;反之,若G_0是树,可选取任意一点做根,并适当指定各边之方向,则得一有向树G。

证明 (1) 因有向树有根,所以G_0是连通的,以下证G_0无回路。

用反证法。设$(v_0,\cdots,v_n)$是G_0中回路,其中$v_0=v_n$,$n\geq 3$。

A. 若 r 在此路中，不妨假设 $v_0=r$，则在 G 中对应 G_0 的边 v_0v_1 的弧一定是从 v_1 到 v_0 的，又因 G 中除根外恰发一弧，所以 G_0 中边 v_1v_2 必是 G 中从 v_2 到 v_1 的弧，…，G_0 中边 $v_{k-1}v_k$ 必是 G 中 v_k 到 v_{k-1} 的弧，…，G_0 中边 $v_{n-1}v_n$ 必是 G 中 v_n 到 v_{n-1} 的弧，而 $v_n=v_0=r$，矛盾。

B. 若 r 不在此回路中，由有向树定义知，v_0 或 v_1 恰发一弧，不妨设 G_0 中的边 v_0v_1 是 G 中从 v_0 到 v_1 的弧，则 $v_0=v_n$ 已发弧，则 G_0 中的边 $v_{n-1}v_n$ 是 G 中从 v_{n-1} 到 v_n 的弧，…，则 G_0 中边 v_1v_2 是 G 中从 v_1 到 v_2 的弧，于是，得 G 中一有向回路，矛盾。

(2) 下面规定各边之方向：

任选树中一点 r 做为根，规定：将 G_0 中边 vv' 改成从 v 到 v' 的弧，当且仅当 $v\neq r$ 且从 v 到 r 的简单路，第一步通过 v'，亦即这条简单路形如 $(v,v',\cdots,r)$

A. 首先证明上述规定无矛盾。即每条边都有方向且方向确定。

对树 G_0 中任意一边 vv'，若 $v'=r$，则按规定，将边 vv' 改成从 v 到 r 的弧，假设 $v'\neq r$，下面证按规定或者从 v 到 v'，或者从 v' 到 v，二者必居其一。

因为从 v,v' 都恰有一条到 r 的简单路 $(v,v_1,v_2,\cdots,r)$，$(v',v_1',v_2',\cdots,r)$，若 $v\neq v_1'$，$v_1\neq v'$，则由于 $v\neq v'$，所以可设 v_i,v_j' 是这两条路中从左向右看第一对相同的点，亦即 $v_i=v_j'$，但是 v，$v_1,\cdots v_i,v_{j-1}',\cdots,v_1',v'$ 互不相同，所以 $(v,v_1,\cdots v_i,v_{j-1}',\cdots,v_1',v',v)$ 是从 v 到自身的简单路，当 $i=j=1$ 时，此路为 (v,v_1,v',v)，长度为 3，即此路是回路，矛盾。

下面证二者恰居其一。

若 $v=v_1'$，且 $v_1=v'$，则 $(v,v',v_2,\cdots,r)$，$(v,v_2',\cdots,r)$，其中 $v'\neq v_2'$，是两条不同的从 v 到 r 的简单路，矛盾。

综上所述，按上述规定，树 G_0 中任意一边都能改成一个有确定方向的弧，亦即，将 G_0 改成了一个有向图 G。

B. 往证 G 是以 r 为根的有向树。

(一) 每一点 v 恰是一弧的起点 $(v\neq r)$。

任取 G 中一点 v，且 $v\neq r$，由于在 G_0 中存在从 v 到 r 的简单路，所以按规定，在 G 中，v 必发弧。若从 v 发两条弧，设这两条弧的终点分别为 v_1,v_1' 且 $v_1\neq v_1'$，则在 G_0 中从 v 到 r 有两条简单路：

$(v,v_1,\cdots,r)$ 和 $(v,v_1',\cdots,r)$，矛盾。

(二) r 不是任意一条弧的起点。

由规定知，此结论显然成立。

(三) r 是根。

对 G 中任意一点 v，在 G_0 中恰有一条从 v 到 r 的简单路。按规定此简单路上诸边的方向都指向 r，故在 G 中，这是一条从 v 到 r 的有向路。

习　题

1. 试举出一个连通的（即漠视为图后是连通的），但无根的有向图。

2. 设 G 是有向图，其中含一有向路 $(e_1,\cdots,e_n)$，其中 $\mathrm{fin}(e_n)=\mathrm{init}(e_1)$，证明：$G$ 不是有向树。

3. 设 G 为有向图，若 G 具有有向树定义中的 1) 和 2)，并且没有有向回路。问：若 G 有限，G 是否是有向树？若 G 不是有限的，如何？

4. 证明：若 r 是有向图 G 的根，则 G 必含有一个以 r 为根的有向支撑树。

§4 Euler 路

定义 设 G 是有向图，G 中一条 Euler 路，就是一条有向路 $(e_1,\cdots,e_n)$，其中 $\text{fin}(e_n)=\text{init}(e_1)$，而且 G 中每条弧在此有向路中恰出现一次。

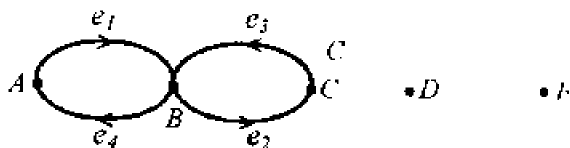


图 4.4.1

注意，Euler 路未必是有向回路，因为它未必是简单的。例如图 4.4.1 中的有向图 G，其中 (e_1,e_2,e_3,e_4) 是 Euler 路，但不是简单有向路。从图 4.4.1 还可看到，G 中的每个点未必在 Euler 路中恰好经过一次；G 中的点可以不在 Euler 路中出现（如图 4.4.1 中的 D、E），也可以出现多次（如点 B）。

Euler 路是一有向图中周游诸弧的路线。一个有向图，如果存在着 Euler 路，就称为 Euler 图。

Euler（1707—1783）是图论的创始人，1736 年，这位瑞士的数学家在图论的第一篇开创性论文中，讨论了一个有趣的问题，即所谓柯尼希斯堡(Konigsberg)城七桥问题。这个城市就是现在的加里宁格勒，位于普列格尔(pregel)河西岸并包括河中的两个岛屿，于是城市就分成了四个部分，各部分通过七座桥来连接，如图 4.4.2(a)所示。这样就产生了一个周游七桥问题：能不能从家里出发，经过七桥恰好一次又回到家里？因为这里的兴趣在于过桥，所以可以把 A,B,C,D 设想成顶点，而把桥画成线，如图 4.4.2(b)所示（这不是图，因为两点间有多条边）。现在的问题就是：能否使图 4.4.2(b)成为一个有向图，而且是 Euler 图？Euler 指出，这是不可能的！Euler 路和 Euler 图因此而得名。



图 4.4.2

定义 设 G 是有向图。G 中点 v 说是孤立的，如果 v 的输入和输出次数全为 0；G 说是平衡的，如果 G 中每点 v，都有有限的输入次数和输出次数，而且输入次数与输出次数相等。

于是，一有限平衡有向图，其弧数有限。显然，一有向图若存在 Euler 路，则必平衡。因为 Euler 路每经过一点 1 次，该点就得到输入次数和输出次数各一次。这样，若一点共被经过 k 次（$k=0$ 时是孤立的），则该点在这有向图中的输入次数和输出次数就都是 k。由此可见，Euler

图中每个点所触及的弧必为偶数条(输入输出各半)。图 4.4.3 是一有限平衡有向图,而(e_{00},e_{01},e_{12},e_{22},e_{21},e_{10},e'_{01},e'_{12},e_{20})是其中的一条 Euler 路。

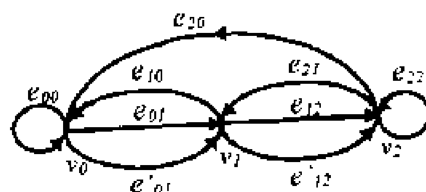


图 4.4.3　一个平衡的有向图

在七桥问题中,图 4.4.2(b)是不可能赋于诸线以方向使成为 Euler 图的,因为其中有些点所触及的线是奇数条(图中 A,B,C,D 所触及的线分别是 5,3,3,3 条,竟全是奇数)。

一个 Euler 图 G,如果没有孤立点,则必强连通。事实上,这时 G 的全部点皆出现在一条有向路 (e_1,e_2,…,e_m)上,即出现在 Euler 路上。其中,$\text{init}(e_1)=\text{fin}(e_m)$。沿着这条路线走两圈,总能够先到达任一给定的顶点 v,然后再到达另一任给的顶点 v'。即对任意的 v,v',都存在从 v 到 v' 的有向通路。

Euler 路实际上是一条一笔画路线。

定理 1(I. J. Good, J. London Math. Soc. 21(1947))　设 G 是无孤立点的有限有向图。于是,G 有 Euler 路当且仅当 G 是平衡的,并且强连通。

证明:必要性显然成立。

充分性,由于 G 没有孤立点,所以 G 的任一点至少发出一条弧,于是 G 中存在至少一条有向路,并且在该有向路中没有弧被重复使用。因为 G 是平衡的,所以 G 中弧数有限,所以这样的路也有限。设 $L=(e_1,\cdots,e_m)$是由无重复弧构成的有向路中的最长者,往证 L 是 Euler 路。

1) 证明 $\text{init}(e_1)=\text{fin}(e_m)$

A. 设 $v=\text{fin}(e_m)$,往证由 v 发出的所有弧都在 L 中。

反证法,若 e 不在 L 中,且 $\text{init}(e)=v$,则(e_1,…,e_m,e)就是一条比 L 更长的由无重复弧构成的有向路,矛盾。

B. 证明由 v 发出的 k 条弧中,必有 e_1,即证:由 v 发出的 k 条弧必有一条排在 L 的最前面。

反证法,若从 v 发出的 k 条弧中无 e_1,则设这 k 条弧是 e_{i1},e_{i2},…,e_{ik},其中 $2\leq ij\leq m$,因为 e_{i1},e_{i2},…,e_{ik}从 v 发出且都在有向路 L 中,则必有 e_{i1-1},e_{i2-1},…,e_{ik-1}射入 v,且 $1\leq ij-1\leq m-1$,即至少有 k 条弧射入 v,这 k 条弧中不包括 e_m,因 e_m 也射入 v,于是至少有 $k+1$ 条弧射入 v,即 v 的输入次数至少是 $k+1$,而输出次数是 k,矛盾。

同理,G 中发到 v 的 k 条弧也都出现在 L 中,并且这 k 条弧中必有 e_m。

所以,在取 L 时,无论哪条弧作为第一条弧,可得 L 是一条从某点出发,到自身的有向路且弧不重复。

2) 证明:G 中所有的弧必恰好在 L 中出现一次。

显然,只须证 G 的每条弧必在 L 中出现即可。

对于 L,若顶点 v 在 L 中,则用 1)中的方法可以证明,从 v 出发到所有弧都在 L 中。

设 e 是 G 的一弧,$u=\text{init}(e)$,任取 L 中一点 v,因为 G 强连通,v,u 间有有向路(e'_1,e'_2,…,

e_1')且 $\text{init}(e_1')=v$，$\text{fin}(e_1')=u$，因 v 在 L 中，e_1' 是由 v 发出的弧，所以 e_1' 在 L 中，因此 $\text{fin}(e_1')=\text{init}(e_2')=v_1'$ 在 L 中，所以 e_2' 在 L 中。同理，e_i' 的终点 u 在 L 中，所以 e 在 L 中。由 e 的任意性知，G 中弧均出现在 L 中。

综上，L 是一条 Euler 路。

推论 设 G 是无孤立点的有限有向图，于是，G 有 Euler 路当且仅当 G 平衡，并且将 G 漠视为图 G_0 时是连通的。

分析定理 1 的证明，不难看到此推论是成立的。

定理 2 设 G 是无孤立点的有限有向图，并且 G 有一条 Euler 路$(e_1,\cdots,e_m)$。令 $r=\text{fin}(e_m)=\text{init}(e_1)$，对每个点 $v\neq r$，令 $e[v]=e_i$，其中 $i=\max\{j\mid \text{init}(e_j)=v\}$。于是，$G$ 的全部点和全部弧$\{e[v]\mid v\neq r\}$做成的有向图 G'，是一个以 r 为根的有向树，即有向支撑树。

证明：由 $e[v]$的定义知：

(1) 对每个点 $v\neq r$，恰有一弧 $e[v]$发出，

(2) r 不发出任何弧。

下面我们证明：

(3) r 是根。

先证 G' 中无有向回路。

若不然，设有一个有向回路$(\cdots,e[v],e[v'],\cdots)$，显然，回路中没有 r，

令 $e[v]=e_j$，$e[v']=e_{j'}$，因为弧 e_j 发到点 v'，而 $v'\neq r$，所以 e_{j+1}是由 v'发出的，但 $e_{j'}$是由 v' 发出的弧中足标最大者，所以 $j<j'$。

而此有向回路又可写成$(e[v'],\cdots,e[v])$

同理得 $j'<j$，矛盾。

下面证对 G 中任一点 v 在 G' 中，有一条从 v 到 r 的有向路。

事实上，在 G' 中，从 v 出发，可以这样走下去

$v\to\text{fin}(e[v])\to\text{fin}(e[\text{fin}(e[v])])\to\cdots$。

因为 G' 中无有向回路，所以此路上点无重复，由于 G' 有限，故最后必然停止在不发弧的点 r 上，所以，r 是根。

定理 3 设 G 是有限平衡有向图，G' 是 G 的有向支撑树，设 G' 的根为 r，G' 中点 $v(\neq r)$发出的弧为 $e[v]$，设 e_1 是 r 在 G 中发出的任一条弧，如果从 e_1 开始任一条有向路 $L=(e_1,\cdots,e_m)$ 满足：

(1) $e_j\neq e_k$，当 $j\neq k$ 时

(2) $e_j=e[v]$当且仅当 $\text{init}(e_j)=v$ 并且 G 中由 v 发出的弧都出现在$(e_1,\cdots,e_j)$中

(3) L 终止在 $e_m\Leftrightarrow G$ 中从 e_m 的终点发出的弧都已经在 L 中出现。

则有向路 L 是一条 Euler 路。

证明：首先证明 $\text{fin}(e)=\text{init}(e_1)=r$

由条件(3)知，由 $r=\text{fin}(e_m)$发出的弧都在 L 中，仿照定理 1 的证明，不难得到结论：$\text{fin}(e_m)$发出的弧中，有一条是 e_1，即 $\text{fin}(e_m)=\text{init}(e_1)$。

其次证明 G 中每条弧恰在 L 中出现一次，由条件(1)知，只须证明 G 中每条弧都出现即可。

反证法，设 G 中弧 e 不在 L 中，令 $\text{fin}(e)=v$，由 G 和 L 的平衡性知，G 中有一条由 v 发出的弧 e'不在 L 中，由于 r 发出的弧都在 L 中，故 $v\neq r$，由条件(2)知，$e[v]$不在 L 中。

同理，当 $\text{fin}(e[v])\neq r$ 时，$e[\text{fin}(e[v])]$不在 L 中，…，于是，得一有向路：$L'=(e,e[v],e[\text{fin}(e[v])],\cdots)$，并且 L'中的弧不在 L 中，L'中的弧都是 G'的弧(除 e 以外)，L'不能无限延长，最终必到达 r，即有一条从 r 发出的弧不在 L 中，与(3)矛盾，所以 G 中弧均出现在 L 中，即 L 是一条 Euler 路。

例如，试看图 3 中有向图 G，命 G'是 G 中由顶点 v_0,v_1,v_2 和 e_{01},e_{21}组成的有向子树(根 $r=v_1$)。从弧 e_{12}出发，可按定理 3 的形成规则得出 Euler 路若干，计有 8 条之多：

$(e_{12},e_{20},e_{00},e'_{01},e_{10},e_{01},e'_{12},e_{22},e_{21})$

$(e_{12},e_{20},e_{00},e'_{01},e'_{12},e_{22},e_{21},e_{10},e_{01})$

$(e_{12},e_{20},e'_{01},e_{10},e_{00},e_{01},e'_{12},e_{22},e_{21})$

$(e_{12},e_{20},e'_{01},e'_{12},e_{22},e_{21},e_{10},e_{00},e_{01})$

$(e_{12},e_{22},e_{20},e_{00},e'_{01},e_{10},e_{01},e'_{12},e_{21})$

$(e_{12},e_{22},e_{20},e_{00},e'_{01},e'_{12},e_{21},e_{10},e_{01})$

$(e_{12},e_{22},e_{20},e'_{01},e_{10},e_{00},e_{01},e'_{12},e_{21})$

$(e_{12},e_{22},e_{20},e'_{01},e'_{12},e_{21},e_{10},e_{00},e_{01})$

§5　Hamilton 路

定义　设 $G=(P,L)$是有限图，$(v_1,\cdots,v_n)$是 G 中一条路。如果 G 中每点恰在此路中出现一次，则称此路为 Hamilton 路；如果 G 中每点，除 v_1 外，恰在此路中出现一次，而 $v_1=v_n$，则此路称为 Hamilton 回路。

定义　设 $G=(P,L)$是有限图，如果 G 中有一条 Hamilton 回路，则称 G 为 Hamilton 图。

例如，

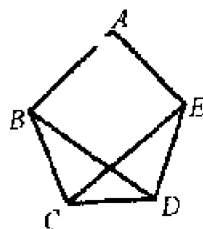


图 4.5.1

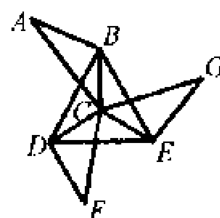


图 4.5.2

图 4.5.1 是 Hamilton 图，它有一条 Hamilton 回路(A,B,C,B,E,A)。图 4.5.2 中有 Hamilton 路，但无 Hamilton 回路，下面我们来说明这个事实。

设图 4.5.2 有 Hamilton 回路 C，遍历所有顶点又回到出发点，则 AC、AB，DF、FC、GC、GE 必在 C 中，则以 C 为端点的三条边出现在回路 C 中，这是不可能的。

关于 Hamilton 路和 Hamilton 回路下面的性质是显然的：

1. 若图中有一点的度为 1，则无 Hamilton 回路。

2. 若图中有一点的度为 0，则既无 Hamilton 路，又无 Hamilton 回路。

3. 设图中有一点的度为 2，若有 Hamilton 回路，则以此点为端点的两条边均出现在此回路中。

4. 设图中有一点的度大于 2，若有 Hamilton 回路，则只用其中的两条边。

例如，我们来说明图 4.5.3 不是 Hamilton 图。

事实上，点 L 的度是 5，若有 Hamilton 回路，只能用以 L 为端点的两条边而抛弃其余的 3 条，对点 H、J 也有类似情况，因此共有从 L，H，J 三点出发的 9 条边，不在 Hamilton 回路中，点 F 的度是 3，Hamilton 回路仅用以 F 为端点的两条边，有一边不在 Hamilton 回路中。同样的情况出现在点 B，D，O，因此，有 4 条以 F，B，D，O 为顶点的边不在 Hamilton 回路中。所以图 4.5.3 中有 13 条边不在 Hamilton 回路中，而此图共有 27 条边，即只有 14 条边可用，图 4.5.3 有 16 个顶点，要够成 Hamilton 回路需要 16 条边，故无法构成 Hamilton 回路，所以图 4.5.3 不是 Hamilton 图。

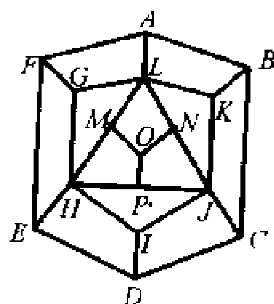


图 4.5.3

和 Euler 路不同，Hamilton 路感兴趣的是图中的点，一条 Hamilton 路决不会在两点间走两次以上，因此，没有必要在有向图中讨论它，只在图中讨论它就可以了。

一个邮递员，如果他的任务需要遍历某些特定的街道，那么他最好走一条 Euler 路；如果他的任务是联系某些特定的收发点，那么他最好走一条 Hamilton 路。

Euler 路同 Hamilton 路相比较，前者要周游诸弧，后者要周游诸点，虽仅有一字之差，但两者的困难程度却不大相同，对于前者，在上节我们已得到了一些较为深刻的定理，比较满意的解决了这个问题；但对于后者，却没有令人满意的结果。寻找一个图是 Hamilton 图的充分必要条件，仍是图论中一个重要问题。

定理 1 如果图 $G=(P,L)$ 是 Hamilton 图，则对 $P(G)$ 的任意一个非空子集 S，都有

$$W(G-S)\leq |S|$$

其中 $|S|$ 表示集合 S 的元数，$G-S$ 表示在 G 中删去 S 中的点以及以 S 中的点为端点的所有边而剩下的图。

证明：设 C 是 G 中的 Hamilton 回路，因为在回路中，依次删去一点及与此点相邻的两条边每次最多只增加一个分支，所以

$$W(C-S)\leq |S|$$

又因为 C 是 G 的支撑子图，所以 $C-S$ 也是 $G-S$ 的支撑子图，故

$$W(G-S)\leq W(C-S)\leq |S|$$

此定理只是判断 Hamilton 图的一个必要条件，通常用它来证明一个图不是 Hamilton 图。例如，将图 4.5.4 中点 A，B，C 的集合记为 S，于是，图 4.5.4 删去 S，剩下的图的分支数

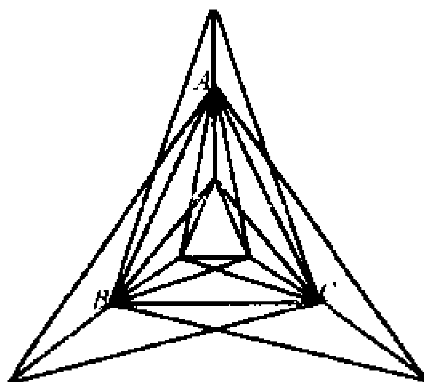


图 4.5.4

是4，即 W(图 4.5.4$-S$)$=4$，而$|S|=3$。由定理 1 知，图 4.5.4 不是 Hamilton 图。定理 1 用于图 4.5.5，图 4.5.6，得不出任何结论。

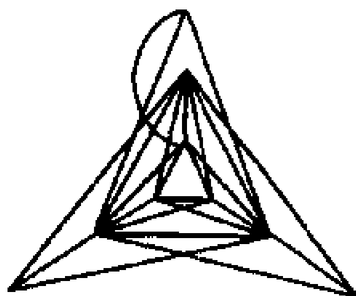


图 4.5.5

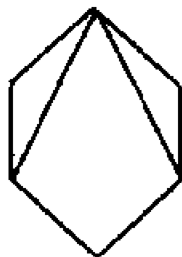


图 4.5.6

定义　设图 G 是非 Hamilton 图，若在 G 中增加任意一条边 uv，$G\cup\{uv\}$ 就变成 Hamilton 图，则 G 称为极大非 Hamilton 图。

定理 2 (Dirac, G. A., 1952)　若 $G=(P,L)$ 是有限图，$|P(G)|\geq 3$，$\delta\geqslant|P(G)|/2$，则 G 是 Hamilton 图。其中 $|P(G)|$ 表示图 G 中点数，δ 表示 G 中点的最小度。

证明：令 $\gamma=|P(G)|$。今后，将一直用 γ 表示 $|P(G)|$。

反证法，即证若 G 是非 Hamilton 图，则在 G 中一定能找到其度$<\gamma/2$ 的顶点。

设 G_0 不是极大非 Hamilton 图，则可以不断地向 G_0 增加若干条边，把 G_0 变成极大非 Hamilton 图 G，显然，对任意点 $v\in P(G)$，$d_{G_0}(v)\leq d_G(v)$，那么，如果在 G 中能找到度$<\gamma/2$ 的点，在 G_0 中也一定能找到。

所以，不妨假设 G 是极大非 Hamilton 图，在 G 中增加一条边，则 $G\cup\{uv\}$ 是 Hamilton 图，于是 $G\cup\{uv\}$ 有 Hamilton 回路 C，在回路中把 uv 删去，变成 G 中一条 Hamilton 路 L，$L=(v_1,v_2,\cdots,v_\gamma)$，其中 $v_1=u$；$v_\gamma=v$。利用 L 做两个集合，令 $S=\{v_i|$边 $v_{i+1}v_1\in L(G)\}$，$i=1,2,\cdots,\gamma-1$，(即如果 $v_1,\cdots,v_\gamma$ 中某 v_j 与 v_1 相邻，则把 v_j 在 L 中前一个顶点放入 S 中)。$T=\{v_i|$边 $v_iv_\gamma\in L(G)\}$，$i=1,2,\cdots,\gamma$。

对点集 S 和 T，我们可以证明 $S\cap T=\phi$，若 $S\cap T\neq\phi$，设 $v_j\in S\cap T$，则 v_{j+1} 与 v_1 相邻，于是

$$(v_1,v_2,\cdots,v_j,v_\gamma,v_{\gamma-1},\cdots,v_{j-1},v_1)$$

是 G 中一条 Hamilton 回路，与 G 不是 Hamilton 图矛盾。

下面证在 G 中能找到其度$<\gamma/2$ 的顶点。

因为 $v_\gamma\notin S\cup T$，故 $|S\cup T|<\gamma$，于是 $d(u)+d(v)=|S|+|T|=|S\cup T|<\gamma$，

从而 u，v 中至少有一点的度$<\gamma/2$，这与 $\delta\geq\gamma/2$ 矛盾，故 G 是 Hamilton 图。

定理 2 无法用于图 4.5.5，图 4.5.6。

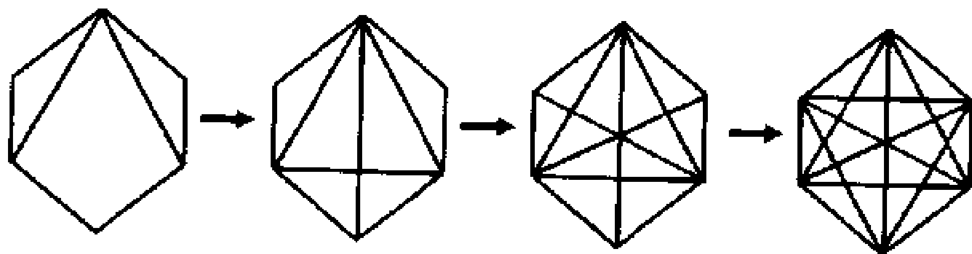
引理 1　设 G 是有限图，u，v 是 G 中任意不相邻的两点，并且满足 $d(u)+d(v)\geq\gamma$，则 G 是 Hamilton 图的充要条件是 $G\cup\{uv\}$ 是 Hamilton 图。

证明：必要性显然。

充分性，若 $G\cup\{uv\}$ 是 Hamilton 图，而 G 不是，仿造定理 2 的证明，得到 $d(u)+d(v)<\gamma$，矛盾。

定义　设 G 是有限图。反复连接 G 中不相邻的并且其度之和不小于 γ 的点对，直到没有这样的点对为止。最后所得之图称为 G 的闭合图，记为 $C(G)$。

例如，得图 4.5.6 的闭合图的过程如下：



引理 2 有限图的闭合图 $C(G)$ 是唯一确定的。

证明：设在 G 中增加边 $l_1,\cdots,l_n$ 后得闭合图 $C_1(G)$，

在 G 中增加边 $f_1,\cdots,f_m$ 后得闭合图 $C_2(G)$。

我们来证明 $C_1(G)=C_2(G)$。

只需证：$\{l_1,\cdots,l_n\}=\{f_1,\cdots,f_m\}$ 即可。

否则，设 l_{k+1} 是第一个不在 $\{f_1,\cdots,f_m\}$ 中的边，设 $l_{k+1}=uv$，做图 $H=G\cup\{l_1,\cdots,l_k\}$，

因为 H 是 $C_2(G)$ 的子图，而 l_{k+1} 不在 $C_2(G)$ 中，所以 $d_H(u)+d_H(v)<\gamma$。

另一方面，因 $G\cup\{l_1,\cdots,l_k\}$ 是 G 的闭合图，所以 $d_H(u)+d_H(v)\geq\gamma$，矛盾，即

$$\{l_1,\cdots,l_n\}\subseteq\{f_1,\cdots,f_m\}，同理，\{f_1,\cdots,f_m\}\subseteq\{l_1,\cdots,l_n\}$$

故 $\{l_1,\cdots,l_n\}=\{f_1,\cdots,f_m\}$

定理 3(Bondy, J. A., Chvatal, V., 1974) 有限图 G 是 Hamilton 图的充要条件是其闭合图 $C(G)$ 是 Hamilton 图。

证明：设图 G 加入边序列 $(l_1,\cdots,l_n)$ 后，得闭合图 $C(G)$。

由引理 1 知，

G 是 Hamilton 图 $\Leftrightarrow G\cup\{l_1\}$ 是 Hamilton 图

$\Leftrightarrow G\cup\{l_1\}\cup\{l_2\}$ 是 Hamilton 图

$\Leftrightarrow\cdots$

$\Leftrightarrow G\cup\{l_1,\cdots,l_n\}$ 是 Hamilton 图

因此，G 是 Hamilton 图当且仅当 $C(G)$ 是 Hamilton 图。

推论 1 设 G 是有限图，若 $C(G)$ 是完全的，则 G 是 Hamilton 图。

此推论可以推导出很多用点的度来表达的关于图是 Hamilton 图的充分条件。例如，当 $\delta\geq\gamma/2$ 时（δ 是图中点的最小度），对于图中任意两点 u，v 都有

$$d(u)+d(v)\geq\gamma$$

故该图的闭合图是完全图，亦即该图是 Hamilton 图。由此可见，Dirac 条件（定理 2）实际上是此推论的一个特例。

用此推论，不难看出图 4.5.6 是 Hamilton 图，而图 4.5.6 是无法使用 Dirac 条件来判定的。故定理 3 强于定理 2。

定理 4 设有限图 G 的度序列（亦即 G 的各点的度，按大小顺序排成的序列）为 $(d_1,d_2,\cdots,d_\gamma)$，其中 $d_1\leq d_2\leq\cdots\leq d_\gamma$，$\gamma\geq3$。如果不存在这样的 m，$m<\gamma/2$，并使得

$$d_m\leq m, d_{\gamma-m}<\gamma-m$$

则 G 是 Hamilton 图。

证明：用反证法，假设 G 不是 Hamilton 图，我们证明在 G 的度序列中可以找到 m，使 $m<\gamma/2$，$d_m\leq m$，$d_{\gamma-m}<\gamma-m$。由定理 3 知，G 的闭合图 $C(G)$ 也不是 Hamilton 图，设 $C(G)$ 中点 u 的度为 $d'(u)$，因为 $C(G)$ 不是 Hamilton 图，所以 $C(G)$ 不是完全图，即 $C(G)$ 中有不相邻的顶

点，设 u,v 在 $C(G)$ 中不相邻且 $d'(u)+d'(v)$ 取最大值，不妨设 $d'(u)\le d'(v)$，因 $d'(u)$ 和 $d'(v)$ 在 $C(G)$ 中不相邻，故 $d'(u)+d'(v)<\gamma$。令 $d'(u)=m$，则 m 就是我们要找的 m，以下证明这个事实。

利用 u,v 做两个集合

$S=\{x|x\in P(G),x$ 在 $C(G)$ 中与 v 不相邻$\}$

$T=\{x|x\in P(G),x$ 在 $C(G)$ 中与 u 不相邻$\}$

则 $|S|=\gamma-d'(v)$，$|T|=\gamma-d'(u)$，集合 $S-\{v\}$ 中点的度都小于等于 $d'(u)$，即 m。

所以 $C(G)$ 中度小于等于 m 的点的个数 $\ge|S-\{v\}|$

$$
\begin{aligned}
&=|S|-1\\
&=\gamma-d'(v)-1\\
&>d'(u)-1 \qquad (\text{因 } d'(u)+d'(v)<\gamma)\\
&=m-1
\end{aligned}
$$

即 $C(G)$ 中度小于等于 m 的点的个数至少为 m。

同理，集合 T 中的度均小于等于 $d'(v)$，

所以 $C(G)$ 中度小于等于 $d'(v)$ 的点的个数 $\ge|T|$

$$
\begin{aligned}
&=\gamma-d'(u)\\
&=\gamma-m
\end{aligned}
$$

又因 $d'(v)<\gamma-d'(u)=\gamma-m$

所以 $C(G)$ 中度小于 $\gamma-m$ 的点的个数至少为 $\gamma-m$

综上，在 $C(G)$ 中度序列 $(d'_1,\cdots,d'_\gamma)$ 有

$$d'_m\le m,d'_{\gamma-m}<\gamma-m$$

由 $d'(u)+d'(v)<\gamma$ 知 $d'(u)<\gamma/2$，所以 $m<\gamma/2$，即存在这样的 m。

因为 G 是 $C(G)$ 的子图，所以在 G 中也存在这样的 m，矛盾。

图 4.5.5 的度序列为：$(d_1,d_2,d_3,d_4,d_5,d_6,d_7,d_8,d_9)=(3,3,3,5,5,6,7,8,8)$，$\gamma=9$，$\gamma/2=4.5$，显然，取 $m=1,2,3,4$，都不能同时满足 $d_m\leqslant m$，$d_{\gamma-m}<\gamma-m$，故由定理 4 知，图 4.5.5 是 Hamilton 图。

图 4.5.6 的度序列为：$(d_1,d_2,d_3,d_4,d_5,d_6)=(2,2,2,3,3,4)$，取 $m=2$，显然，$m<\gamma/2$，$d_2\le2$，$d_4<4$。故定理 4 无法判定图 4.5.6 是否是 Hamilton 图。

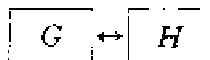
可见，定理 4 强于定理 2，但不强于定理 3。

定义　实数序列 $(p_1,\cdots,p_n)$ 称为由实数序列 $(q_1,\cdots,q_n)$ 所增大，如果 $p_i\leqslant q_i$，$i=1,\cdots,n$。

例如，(2,2,2,2,2) 由 (2,2,2,3,3) 所增大。

定义　设 G、H 是有限图，G 称为由 H 所度增大，如果 $|P(G)|=|P(H)|$，并且 G 的不减度序列由 H 的不减度序列所增大。

定义　设 G、H 是两个无公共点的有限图，将 G 的每个点和 H 的每个点都用边连接起来得到的图，称为 G 与 H 的连接图，记为：



例如

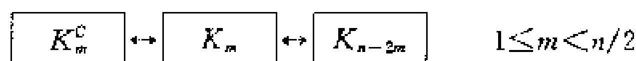


定义　设 G,H 是两个有限图，如果 $P(G)=P(H)$，并且对 G、H 中任意两点 u、v，u 和 v 在 G 中相邻当且仅当它们在 H 中不相邻，则称 G 是 H 的补图，H 是 G 的补图，可以将 G 记为 H^C，也可将 H 记为 G^C。

例如，下面的两个图就是互为补图。



用 K_m 表示由 m 个点组成的完全图，将如下三个图：



从左到右顺序连接起来构成的连接图记为 $C_{m,n}$。

例如，图 $C_{1,5}$、$C_{2,5}$ 分别如下：



引理 3　若 $1<m<n/2$，则图 $C_{m,n}$ 是非 Hamilton 图。

证明：图 $C_{m,n}$ 中 K_m 部分有 m 个点，令 S 是这 m 个点组成的集合，于是

$$W(C_{m,n}-S)=W(K_m^C)+W(K_{n-2m})$$
$$=m+1>|S|$$

由定理 1，$C_{m,n}$ 是非 Hamilton 图。

定理 5(Chvatal)　若 G 为非 Hamilton 图，$\gamma>3$，则 G 由某个 $C_{m,\gamma}$ 所度增大。其中 γ 是 $P(G)$ 的元数。

证明：设 G 的不减度序列为 $(d_1,d_2,\cdots,d_\gamma)$。由定理 4 知，存在 $m<\gamma/2$，使得 $d_m\leq m$，$d_{\gamma-m}<\gamma-m$。故 $(d_1,d_2,\cdots,d_\gamma)$ 由序列：

$$(m,\cdots,m,\gamma-m-1,\cdots,\gamma-m-1,\gamma-1,\cdots,\gamma-1)$$

所增大，其中度 m 有 m 个，度 $\gamma-m-1$ 有 $\gamma-2m$ 个，度 $\gamma-1$ 有 m 个。

显然，后一个序列正是图 $C_{m,\gamma}$ 的度序列，故 G 由 $C_{m,\gamma}$ 所度增大。

下面我们来看一下流动推销员问题：

在§2 中，我们给出了世界六大城市之间的交通网，一个流动推销员希望访问这六个城市，最后再回到出发点，怎样安排旅行最节省时间？

这是在一个带权的完全图中求一条有最小权的 Hamilton 回路问题，对于求这种所谓最优 Hamilton 回路问题，目前尚没有一个好的解决方法。下面介绍的方法，只能求出较好的 Hamilton 回路。

1. 首先求出一条 Hamilton 回路 C。

2. 用下面方法修改 C，以得到更小权的 Hamilton 回路，

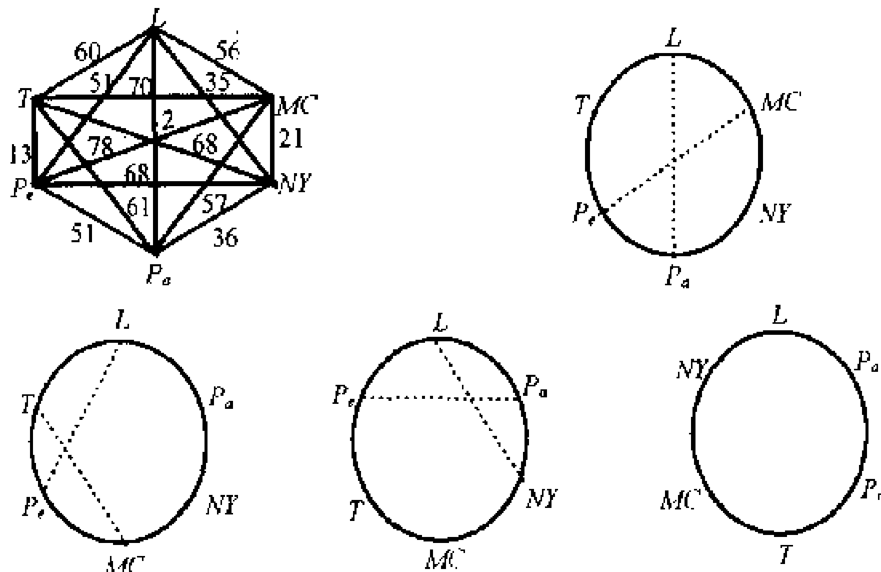
设 $C=(v_1,v_2,\cdots,v_7,v_1)$，如果 $i+1<j$，并且

$$w(v_iv_j)+w(v_{i+1}v_{j+1})<w(v_iv_{i+1})+w(v_jv_{j+1})$$

则 Hamilton 回路 $C_{i,j}$：

$$C_{i,j}=(v_1,v_2,\cdots,v_i,v_j,v_{j-1},\cdots,v_{i+1},v_{j+1},v_{i+2},\cdots,v_7,v_1)$$

就是 C 的一个改进。



一个较好的 Hamilton 回路是：从伦敦出发，依次经过巴黎，北京，东京，墨西哥，纽约，最后再回到伦敦。

§6　König 无限性引理

无限性引理（König D. Fundamenta Math. 8(1926)，114—134）　设 G 为一有向树，有根 v_0，有无限多个点，但每个点的（输入）次数皆有限（除了根的输出次数为 0，其它诸点输出次数为 1）。于是，G 就有一条由根 v_0"起源"的无限的路，即一个无限的点序列

$$v_0,v_1,v_2,\cdots$$

其中 $\text{fin}(e[v_{j+1}])=v_j$，对所有 $j\geq 0$。简言之，在一个其点之次数有限的无限有向树中，必有一源于根的无限路

$$v_0 \leftarrow e[v_1] \text{---} v_1 \leftarrow e[v_2] \text{---} v_2 \leftarrow e[v_3] \text{---} v_3 \quad \cdots$$

证明：对于有向树，我们把根看成诸点的祖宗。若 v 是由 v' 发出的弧 $e[v']$ 的终点，就是说 v 是 v' 的父亲，v' 是 v 的儿子。"起源"的说法就是这个意思。注意，这与弧中箭头的方向正好相反，由 v' 发出到 v，反而说 v' 由 v 起源。

从 v_0 开始，找一无限路如下：对 $j\geq 0$ 用归纳法。假设 v_j 已找到，它有无限多个后代。这样，一方面因所设 v_j 的次数有限，即 v_j 只有有限多个儿子 $u_1,\cdots u_n$；另一方面因 v_j 有无限多个后代，故 v_j 的诸儿子中至少有一个也有无限多个后代，命这样的一个儿子为 v_{j+1}。如此类推，就得到一条无限的路

$$(v_0,v_1,v_2,\cdots)$$

无限性引理证毕。

König 因此指出：如果人类永不灭绝，那么现在就有一个活着的人一直延续他的后代。

事实上，就从现在活着的几十亿人开始算，年复一年地繁殖下去，既然人类永不灭绝，故随着时间的无限延续，就得到无限多个人，包括从现在开始往后死去的人在内。这无限多个人无非是现在活着的有限多个人（以及他们）的后代，所以必有一个现在活着的人有着无限多个后代。好了，把人看成是有向树的点，那么，一个人和他的无限多个后代就是一株无限的有向树，这个人就是这株有向树的根。因为每个人只能有有限个儿子，所以这株树中每个点的输入次数皆有限。于是，根据无限性引理，必有一源于此根的无限路。也就是说，这个人一直延续他的后代。

推论 1 设有一计算机算法 R，它反复地分化成有限个子算法（即算法分成子算法，子算法又分成子子算法，…）。如果每条子算法的链都最后终止，则本算法 R 也终止（即不再延续它的代代分化）。

推论 2 设 S 是正整数序列

$$(x_1,x_2,\cdots,x_n),n\geq 0$$

的集合，它适合条件

(1) 若 $(x_1,x_2,\cdots,x_n)\in S$，则其"前段" $(x_1,x_2,\cdots,x_k)\in S$，对于 $0\leq k\leq n$；

(2) 若 $(x_1,x_2,\cdots,x_n)\in S$，则只存在有限多个 x_{n+1} 使 $(x_1,\cdots,x_n,x_{n+1})\in S$。简言之，在 S 中，每个元素 $(x_1,x_2,\cdots,x_n)$ 只有有限多个"后随" $(x_1,\cdots,x_n,x_{n+1})$；

(3) 不存在那样的无限序列 $(x_1,x_2,\cdots)$，它的所有"前段" $(x_1,x_2,\cdots,x_n)$ 全在 S 中。

那么，S 必为一有限集合。

事实上，把 S 中的元素看成点，把"后随"看成"儿子"，这样 S 就是一个有向图。根是长度为 0 的空序列（ ），由(2)知它有有限个儿子 (x_1)，每个儿子 (x_1) 又有自己的有限个儿子 (x_1,x_2)，…。条件(2)是说 S 的每个顶点次数皆有限。由(1)可知 S 中除根（ ）外每个顶点 $v=(x_1,x_2,\cdots,x_n)$ 都有唯一的"父亲" $(x_1,\cdots,x_{n-1})$，有唯一指向它"父亲"的弧 $e[v]$，有唯一的通到它"祖宗"（ ）的路。故 S 为一有向树。而(3)是说 S 中没有源于根的无限路。由无限性引理，即知 S 必为一有限集合。

利用无限性引理，王浩成功地解决了用骨牌来砌出整个平面的问题。一张骨牌就是一个正方形，由它的两条对角线将其分成了 4 个小三角形，每个小三角形里都刻有确定的数，如图 4.6.1 所示。

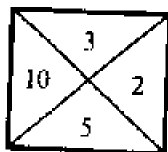


图 4.6.1

砌平面的问题是：要用有限张骨牌（每张可无限地重复）布满整个平面（不许转动或反射每张骨牌面上的 4 个值），使两张相邻的骨牌在接处都有相同的值。例如，用图 4.6.2 的六张牌确实是可以砌出整个平面的，其实是通过图 4.6.3 的"2×3"长方形的一再重复，就可以砌出整个平面来。

读者不难验证，用图 4.6.4 中的三张骨牌是无论如何也砌不出整个平面的。

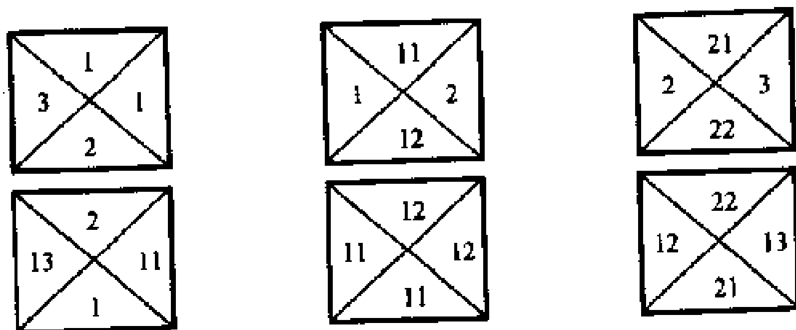


图 4.6.2

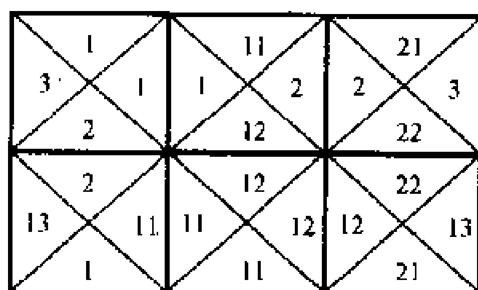


图 4.6.3

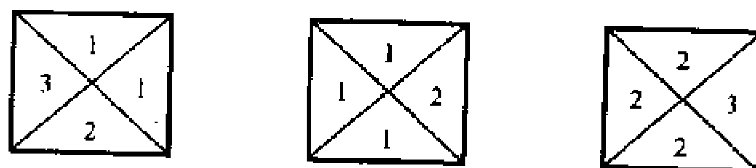


图 4.6.4

王浩定理(Sci,Am. 213(1965),98—106)　只要能砌出第一象限，就能砌出整个平面。

证明：既然能砌出第一象限，那么对所有 n 均能砌出 $2n\times 2n$ 的正方形：

$$0\times 0,2\times 2,4\times 4,6\times 6,8\times 8,\cdots。$$

把 $2n\times 2n$ 正方形的砌法看成是 $(2n+2)\times(2n+2)$ 正方形的砌法的父亲，如果后者可通过前者镶边得出。这样，我们就得到一棵有向树，其根为 0×0 正方形，因能砌出第一象限，故这棵树有无限个点，又因有有限张骨牌，所以镶边的方法是有限的，所以每个点只有有限个儿子。于是，根据无限性引理，这棵树必有一条源于根的无限路，也就是说，从 (0×0) 开始，可逐步地通过镶边而砌出整个平面来。

习　　题

1. 试证若允许转动骨牌，则砌平面问题无条件地可解。
2. 若允许使用无限张骨牌，请举出一个能砌成第一象限，却砌不成整个平面的例子。

第五章 整 数

本章介绍"数论"中一些最基本的事实，就是说，介绍整数的一些最基本的性质。我们设这一章，一方面是由于其本身的重要性，另一方面是为下面三章作准备，因为，下面三章里一些较抽象的内容很多都可以在数论中找到根源和实例。

我们知道，任意两个整数可以相加，相减，相乘，结果仍是整数。但两个整数不一定能在整数的范围内相除，这是整数系统的特点，它和有理数系统及实数系统等不一样，既然如此，研究整数就必须针对这一特点加以分析，实际上，研究整数的性质基本上就是要研究整除性和因数分解等问题以及其它一些有关的问题。

本章中，有时似乎在叙述或证明一些尽人皆知非常明显的事实。实则并非如此。有些事情，我们习而不察，知其然而不知其所以然。有些事情，虽然知道，却知道得不确切。

本章中，若未特别指明，凡出现的数都是整数。

§1 整除性 辗转相除

带余除法定理 对任意整数 a 和 $b(b\neq 0)$，唯一存在一对数 q 和 r，使得 $a=qb+r$ 且 $0\leq r<|b|$，其中 q 称为商数，r 称为余数。

证明：A. 当 $b>0, a\geq 0$ 时，我们利用长除法可求出 q 和 r，存在性成立。

B. 当 $b>0, a=-a'<0$，于是，根据 A 可求得 q', r' 使得

$$a'=q'b+r', 0\leq r'<b$$

即 $a=(-q')b+(-r')$

若 $r'=0$，则取 $q=-q', r=0$，存在性成立；

若 $r'>0$，取 $r=b-r'$，于是

$$a=(-q'-1)b+r, 0<r<b$$

故取 $q=-q'-1$，则存在性成立。

C. 当 $b=-b'<0$，而 a 任意时，由 A，B 可求得 q', r' 使

$$a=q'b'+r', 0\leq r'<b'$$

这时只要取 $q=-q', r=r'$，则存在性成立，

由 A、B、C 知，对任意 $a, b(b\neq 0)$，有

$$a=qb+r, \quad 0\leq r<|b| \tag{1}$$

D. 最后证唯一性。

设另有一对 q', r' 满足

$$a=q'b+r' \quad 0\leq r'<|b| \tag{2}$$

(2)－(1)得
$$r'-r=b(q-q') \tag{3}$$

从而
$$|r'-r|=|q-q'||b| \tag{4}$$

注意到 $|r'-r|<|b|$，而 $|q-q'|\geq 0$ 且为整数，得 $q=q'$，从而 $r=r'$。

定义 设 a, b 是两个整数，如果有整数 c 存在，使得

$$a=bc \tag{5}$$

则我们说 a 是 b 的倍数，b 是 a 的因数，或说 a 被 b 整除，b 整除 a，记作 $b|a$。

由定义，±1 整除任意整数，而任意整数整除 0，特别 $0|0$。

$b\neq0$ 时，$b|a$ 等于说有理数 $\frac{a}{b}$ 是整数。事实上，若 $\frac{a}{b}$ 等于整数 c，则此 c 便适合(5)；反之，若整数 c 适合(5)，则 $\frac{a}{b}=c$，因而 $\frac{a}{b}$ 是整数。

$b\neq0$ 时，$b|a$ 又等于说以 b 除 a 所得的余数为 0。事实上，若(1)中的 $r=0$，则取 $c=q$，(5)便成立；反之，若(5)成立，则由商及余数的唯一性，必有 $q=c$，$r=0$。

关于整数有下面几条性质：

1. 若 $a|b$，$b|c$，则 $a|c$

证明：因为 $a|b$，$b|c$，故有整数 d，e 使得

$$b=ad,\ c=be$$

所以 $c=ade$，又因 de 是整数，所以 $a|c$。

2. 若 $a|b$，则 $a|bc$

证明：因为 $a|b$，所以存在整数 d，使得

$b=ad$，故 $bc=adc$，又因 dc 是整数，所以 $a|bc$。

3. 若 $a|b$，$a|c$，则 $a|b\pm c$。

证明：因为 $a|b$，$a|c$，则存在整数 d，e 使得

$b=ad$，$c=ae$，所以 $b\pm c=a(d\pm e)$

又因 $d\pm e$ 为整数，所以 $a|b\pm c$。

4. 若 a 整除 $b_1,\cdots,b_n$，则 $a|\lambda_1b_1+\cdots+\lambda_nb_n$。

证明：因为 $a|b_i$，由 2，则 $a|\lambda_ib_i$，再由 3，$a|\lambda_1b_1+\lambda_2b_2$，由此及 $a|\lambda_3b_3$，又有 $a|\lambda_1b_1-\lambda_2b_2+\lambda_3b_3$，…

如此类推，便证明了，$a|\lambda_1b_1+\cdots+\lambda_nb_n$。

5. 若在一等式中，除某项外，其余各项都是 a 的倍数，则此项也是 a 的倍数。

证明：设等式为 $b-c=-d+e+f$，其中 b，c，d，f 都是 a 的倍数，于是 $e=b-c-d-f$，由 4，

$a|b-c+d-f$，所以 $a|e$，即 e 也是 a 的倍数。

6. 若 $a|b$，$b|a$，则 $b=\pm a$。

证明：若 $a=b=0$，则 $b=\pm a$ 显然是对的，设 a，b 不都是 0，不妨设 $a\neq0$，因为 $a|b$，$b|a$，故存在整数 d，e 使 $b=ad$，$a=be$，从而 $a=ade$，于是 $de=1$，因 d，e 分别为整数，而相乘又得 1，故此二数必然都是 ±1，因而 $b=\pm a$。

定义　若 d 是 a 的因数也是 b 的因数，则 d 说是 a，b 的公因数。

7. 设 $a=qb+c$

于是 a，b 的公因数和 b，c 的公因数是完全相同的。

证明：若 d 是 b，c 的公因数，由 5，则 d 也是 a 的因数，故 d 是 a，b 的公因数；

若 d 是 a，b 的公因数，由 5，则 d 也是 c 的因数，故 d 是 b，c 的公因数。

定义　若 d 是 a，b 的公因数，而 a，b 的任意公因数整除 d，则 d 说是 a，b 的最高公因，记作 $d=(a,b)$。

这个定义只是说，如果有那样的 d，则 d 叫做 a，b 的最高公因。对于任意 a，b 是否有那样的 d 呢？现在还不知道，下面再研究。不过，有一点是容易说明的：如果 a，b 有最高公因，则最

高公因除符号外唯一确定。事实上，若 d 和 d' 都是 a,b 的最高公因，则 $d|d'$，$d'|d$，因而由 6，$d'=\pm d$。

现在我们来看，是否任意 a,b 有最高公因？若 $b|a$，则由定义易见，b 就是 a、b 的最高公因。同样，$a|b$ 时 a 就是 a,b 的最高公因。

今设 a 不整除 b，b 不整除 a，因为任意整数整除 0，所以 $a\neq 0$，$b\neq 0$，以 b 除 a 得商 q_1、余数 r_1，以 r_1 除 b 得商 q_2，余数 r_2，以 r_2 除 r_1 得商 q_3，余数 r_3，依此类推有下列各式：

$$
\begin{aligned}
a &= q_1b + r_1 \\
b &= q_2r_1 + r_2 \\
&\ \,\vdots \\
r_{k-2} &= q_kr_{k-1} + r_k \\
&\ \,\vdots \\
r_{n-2} &= q_nr_{n-1} + r_n \\
r_{n-1} &= q_{n+1}r_n
\end{aligned}
$$

因 $r_1,\cdots,r_n,\cdots$ 逐次减小，所以一直做下去必然减到 0，如最后一式所示，由 7，a,b 的公因数和 b,r_1 的公因数完全相同，b,r_1 的公因数又和 r_1,r_2 的公因数完全相同，依此类推，知 a,b 的公因数和 r_{n-1},r_n 的公因数完全相同，而 $r_n|r_{n-1}$，故 r_n 是 r_{n-1},r_n 的最高公因，因而也是 a,b 的最高公因，这样，我们就证明了：

定理 1 任意二整数 a,b 有最高公因。

上面求最高公因的方法叫辗转相除。

定理 2 a,b 的最高公因 d 可以表为 a,b 的倍数和，即表为下面的形式：

$$d = sa + tb$$

其中 s,t 都是整数。

证明：若 a,b 中有一个整除另一个，不妨假设 $b|a$，则 $d=b=0a+1b$，得证。

现设 a 不整除 b，b 不整除 a，由辗转相除得

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} b \\ r_1 \end{pmatrix}$$

$$\begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$$

依此类推

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix}$$

设
$$A = \begin{pmatrix} T_k & V_k \\ S_k & U_k \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$$

则
$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} T_k & V_k \\ S_k & U_k \end{pmatrix}\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix}$$

$$A^{-1}=\frac{1}{|A|}A^{*} \qquad A^{*}\text{为伴随矩阵}$$
$$=\frac{1}{|A|}\begin{pmatrix} U_k & -V_k \\ -S_k & T_k \end{pmatrix}$$

因为 $\begin{vmatrix} q_1 & 1 \\ 1 & 0 \end{vmatrix}=\cdots=\begin{vmatrix} q_k & 1 \\ 1 & 0 \end{vmatrix}=1$

所以 $|A|=(-1)^k$

故 $A^{-1}=\begin{pmatrix} \frac{U_k}{(-1)^k} & \frac{-V_k}{(-1)^k} \\ \frac{-S_k}{(-1)^k} & \frac{T_k}{(-1)^k} \end{pmatrix}=\begin{pmatrix} (-1)^k U_k & (-1)^{k-1}V_k \\ (-1)^{k-1}S_k & (-1)^k T_k \end{pmatrix}$

即 $\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix}=A^{-1}\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} (-1)^k U_k & (-1)^k V_k \\ (-1)^{k-1}S_k & (-1)^k T_k \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}$

得 $r_k=(-1)^{k-1}S_k a+(-1)^k T_k b$

取 $k=n$，则因 r_n 即为最高公因 d，得

$$d=(-1)^{n-1}S_n a-(-1)^n T_n b$$

这表明，任给两个数，我们都可将它们的最高公因表为它们的倍数和的形式，这里需求出 n, S_n, T_n。

为能简便地计算它们，让我们看下面的等式：

$$\begin{pmatrix} T_k & V_k \\ S_k & U_k \end{pmatrix}=\begin{pmatrix} T_{k-1} & V_{k-1} \\ S_{k-1} & U_{k-1} \end{pmatrix}\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} q_k T_{k-1}+V_{k-1} & T_{k-1} \\ q_k S_{k-1}+U_{k-1} & S_{k-1} \end{pmatrix}$$

得 $U_k=S_{k-1}$　　　$V_k=T_{k-1}$

即 $U_{k-1}=S_{k-2}$　　　$V_{k-1}=T_{k-2}$　　　(1)

而 $S_k=q_k S_{k-1}+U_{k-1}$　　　$T_k=q_k T_{k-1}+V_{k-1}$　　　(2)

所以 $S_k=q_k S_{k-1}+S_{k-2}$　　　$T_k=q_k T_{k-1}+T_{k-2}$　　　(3)

(1)式在 $k>2$ 时成立，(2)式在 $k\geq 2$ 时成立，所以(3)式在 $k>2$ 时成立。

现令 $S_0=U_1$，　$T_0=V_1$

则(1)在 $k=2$ 时也成立，即(3)在 $k=2$ 时也成立。

由 $\begin{pmatrix} T_1 & V_1 \\ S_1 & U_1 \end{pmatrix}=\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}$

得 $S_0=0, S_1=1, T_0=1, T_1=q_1$

根据这个初值及(3)式，便可求出任意的 S_k, T_k。

例如，求 301 和 133 的最高公因并表为它们的倍数和。

解：用辗转相除法求最高公因逐次得商及余数并计算 S_k、T_k 如下表所列：

k	0	1	2	3	4
r_k		35	28	7	0
q_k		2	3	1	4
S_k	0	1	3	4	
T_k	1	2	7	9	

因此,最高公因为 7,表为原二数的倍数和如下:

$$
\begin{aligned}
7 &= (-1)^2 \times 4 \times 301 + (-1)^3 \times 9 \times 133 \\
&= 4 \times 301 + (-9) \times 133
\end{aligned}
$$

习　　题

1. 求证任意奇数的平方减 1 必是 8 的倍数。

2. 求 1331 和 5709 的最高公因并表为其倍数和。

3. 记 T_k 如下:

$$T_k = [q_1, q_2, \cdots, q_k]$$

求证

$$S_k = [q_2, \cdots, q_k]。$$

4. 求证

$$[q_1, q_2, \cdots, q_k] = [q_k, \cdots, q_2, q_1]。$$

5. 定义两数的最低公倍。试证若 d 和 m 分别是 a,b 的最高公因和最低公倍且四数皆非负,则

$$dm = ab$$

6. 表演者请观众随意写一个相当大的数,任意颠倒其各位数字,所得的数和原数相减,然后任意删去一个非 0 数字,把结果告诉表演者。表演者把此数输入计算机,计算机就知道删去的数字是什么并加以显示。例如,观众写的数是 3208754,颠倒各位数字变为 8047325,相减得 4838571。假定观众删去数字 7,结果成为 483851。表演者把此数输入计算机,计算机立即显示出数字 7 给观众看!表演者当然是在计算机内预先埋伏下一个程序。试编出一个这样的程序。

§2　互质　质因数分解

定义　若 a,b 除 ± 1 外无其它公因数,则我们说 a 和 b *互质*。

显然,a 和 b 互质当且仅当 $(a,b)=1$;± 1 和任意整数互质。

定理 0　a,b 互质当且仅当存在 s,t 使 $sa+tb=1$。

证明:必要性显然。

充分性,若不然,设 $d=(a,b)>1$,则

$$d|a, d|b$$

所以,$d|1$,矛盾。

定理 1　若 $(a,b)=1$ 且 $a|bc$,则 $a|c$。

证明:因为 $(a,b)=1$,所以存在 s,t 使 $sa+tb=1$

即 $sac+tbc=c$,故 $a|c$。

定理 2　若 b 和 $a_1, a_2, \cdots, a_n$ 都互质,则 b 和 $a_1 a_2 \cdots a_n$ 互质。

证明:由已知得,对 $i=1,2,\cdots,n$,有 s_i, t_i 使

$$s_i b + t_i a_i = 1$$

将这 n 个式子乘起来,左边有 2^n 项,其中有一项包含 $a_1 a_2 \cdots a_n$,而其余各项都包含 b,所以,相乘后得式如下:

$$Sb + T a_1a_2\cdots a_n = 1$$

所以 b 和 $a_1a_2\cdots a_n$ 互质。

定理 3　若 $m_1,m_2,\cdots,m_k$ 两两互质而都整除 a，则 $m_1m_2\cdots m_k | a$。

证明：用归纳法证明。

当 $k=1$ 时，显然成立。

设对 $1\leq i<k$ 的 i 成立，往证 $i+1$ 时成立。

已知：$m_1m_2\cdots m_i|a$，所以 $a= m_1m_2\cdots m_iq$

由定理 2 知，m_{i+1}和 $m_1m_2\cdots m_i$ 互质，又因 $m_{i+1}|a$，再由定理 1 知，

$$m_{i+1}|q,$$

于是 $q=m_{i+1}p$，即 $a= m_1m_2\cdots m_im_{i+1}p$

所以 $m_1m_2\cdots m_{i+1}|a$

综上所述，本定理成立。

定义　一个正整数，如果不等于 1 而且除了自己和 1 外没有其它正因数，则这个正整数称为一个质数。

定义　能表成大于 1 的两个正整数积的数称为合数。

显然，1 即不是质数也不是合数；任意两质数互质。

下面我们来说明质数 p 与整数 a 互质的充分必要条件是 p 不整除 a。

必要性，事实上，若 $p|a$，则 p 和 a 除±1 外还有公因数$\pm p$，故二者不互质，矛盾。

充分性，若 p 不整除 a，p 只有$\pm p$ 和±1 为其因数，而 p 不整除 a，所以只有±1 为 p，a 的公因数，所以二者互质。

定理 4　若质数 p 整除 $a_1a_2\cdots a_n$，则 p 整除 $a_1,a_2,\cdots,a_n$ 之一。

证明：若 $a_1,a_2,\cdots,a_n$ 都不能被 p 整除，则 p 和它们都互质，故由定理 2，p 和它们的乘积互质，因而 p 将不能整除此乘积。

定理 5（算术基本定理）　任意正整数 $n(n\neq1)$恰有一法写成质数的乘积。

证明：(1) 先证 n 可以写成质数的乘积。用数学归纳法。

当 $n=2$ 时，因为 2 是质数，算是已经写成了质数的乘积。

设 $n<a$ 时 n 可以写成质数的乘积，试证 $n=a$ 时也可以这样写。

若 a 是质数，则 a 算是已经写成了质数的乘积；

若 a 不是质数，于是，a 有因数 b，$1<b<a$。设 $a=bc$，则 $1<c<a$。由归纳假设，b 和 c 都可以写成质数的乘积，但 $a=bc$，只要把这两个乘积接起来就把 a 写成了质数的乘积。

综上所述，对任意正整数 $n(n\neq1)$可以写成质数的乘积。

(2) 唯一性

若 $n=p_1\cdots p_h(p_1\leq p_2\leq\cdots\leq p_h)$

$\quad=q_1\cdots q_k(q_1\leq q_2\leq\cdots\leq q_k)$

往证：$h=k$ 且 $p_i=q_i$。

由于 $p_1\cdots p_h= q_1\cdots q_k$，　　(＊)

则得 $p_1|q_1\cdots q_k$，

由定理 4，$p_1|q_i$得 $q_i=p_1$

所以 $q_1\leq p_1$

同理：$p_1\leq q_1$故 $p_1=q_1$

在(＊)式的两边消去 p_1 得 $p_2 \cdots p_h = q_2 \cdots q_k$

如此进行下去，可得 $p_1,\cdots,p_h$ 和 $q_1,\cdots,q_k$ 完全相同，不存在等式的一边消完而另一边还剩下质数的情况，因为一些质数之积不可能等于 1，所以 $h=k$ 且 $p_i=q_i$。

推论 1 任意整数($\neq 0,\neq \pm 1$)恰有一法写成下面的形式：

$$\pm p_1 \cdots p_k$$

其中 $p_1,\cdots,p_k$ 都是质数。

$p_1,\cdots,p_k$ 中可能有的质数重复出现，若把相同的质数归在一起，则有

推论 2 任意整数($\neq 0,\neq \pm 1$)恰有一法写成下面的形式：

$$\pm p_1^{r_1} \cdots p_n^{r_n}$$

其中 $p_1,\cdots,p_n$ 是不同的质数，$r_1,\cdots,r_n$ 是正整数。

定理 6(欧几里得) 质数无穷多。

证明：用反证法，假定质数只有有限个，命为 $p_1,p_2,\cdots,p_n$。

试看 $N=p_1p_2\cdots p_n+1$，则 N 应为非质数，但是 p_i 不整除 N，故 N 无质因数，此不可能。结论得证。

习　题

1. 求证§1 中 S_k,T_k 互质。

2. 说明任意有理数($\neq 0,\neq \pm 1$)恰有一法写成下面的形式：

$$\pm p_1^{r_1} \cdots p_n^{r_n}$$

其中 $p_1,\cdots,p_n$ 是不同的质数，$r_1,\cdots,r_n$ 是非 0 整数。

3. 设整数 a 写成了推论 2 中的形式，a 有多少个因数？

4. 设 $a=\pm p_1^{r_1}\cdots p_n^{r_n}$，$b=\pm p_1^{s_1}\cdots p_n^{s_n}$，其中 $p_1,\cdots,p_n$ 是不同的质数，$r_1,\cdots,r_n,s_1,\cdots,s_n$ 是非负整数(事实上，任意两个非 0 整数 a,b 一定可以写成这样，因为总可以在 a,b 的分解式中添上一些质数的 0 次方而把两个分解式中出现的质数凑成都是 $p_1,\cdots,p_n$)。问：a,b 的最高公因和最低公倍是什么？

5. 按照下列提示，不借助于最高公因的理论直接用数学归纳法证明算术基本定理(Zermelo 证法)：设定理对小于 a 的数成立，试证对于 a 成立。取 a 的大于 1 的最小的因数 p，易见 p 是质数，因之，$a=pb$，由此易证 a 可以分为质因数的乘积，假定 a 尚有另一种分法，此分法中必不含 p，设 q 是其中的一个质因数，则 $a=qc$，试看

$$a_0 = a - pc = p(b-c) = (q-p)c。$$

$a_0,b-c,q-p,c$ 都是小于 a 的正数，由此及上式不难推出矛盾。

6. 求证等差级数

$$7,11,15,\cdots$$

中有无穷多个质数。提示：易证任意多个形为 $4n+1$ 的数相乘仍是 $4n+1$ 的形式。假定上面等差级数中只有有限个质数 $p_1,\cdots,p_m$，试看 $N=4p_1\cdots p_m-3$。

7. 求证有无穷多个质数形为 $6n+5$。

8. 试编一个分解一数为质因数的程序。

§3 合　　同

定义　设 m 是正整数，a,b 任意，若 $m|(a-b)$，称 a 合同 b 模 m，或称关于模 m，a 与 b 同余，记为 $a\equiv b(\mathrm{mod}\ m)$。

容易证出，$a\equiv b(\mathrm{mod}\ m)$ 的充要条件是 m 去除 a,b 所得余数相同。

事实上，设 $a=q_1m+r_1, 0\leq r_1<m$；

$b=q_2m+r_2, 0\leq r_2<m$。

于是　　$a-b=(q_1-q_2)m+(r_1-r_2)$，

故 $m|(a-b)$ 的充要条件是 $m|r_1-r_2$，但 $|r_1-r_2|<m$，

所以 $m|(a-b)$ 的充要条件是 $r_1-r_2=0$，

即 $r_1=r_2$。

所谓合同，不过是整除性的一种表达方式，但这种说法有好处，因为以下可以看出，数的合同和数的相等类似，因而可以用我们较为熟悉的相等的观点来处理整除性的一些问题。

因为模 m 合同等于说以 m 来除所得的余数相同，所以 mod m 下面的三个简单事实成立：

1°　$a\equiv a$；

2°　若 $a\equiv b$，则 $b\equiv a$；

3°　若 $a\equiv b, b\equiv c$，则 $a\equiv c$；

由此可以看出合同是一种等价关系。

4°　若 $a\equiv b, c\equiv d$，则 $a\pm c\equiv b\pm d, ac\equiv bd$；

证明：由题设有 r,s 使 $a-b=rm, c-d=sm$，

故 $(a\pm c)-(b\pm d)=(r\pm s)m$，因而 $a\pm c\equiv b\pm d$。

其次，$ac=(b+rm)(d+sm)=bd+rdm+bsm+rsm^2\equiv bd+0+0+0=bd$，故 $ac\equiv bd$。

由 4°，在一个合同式中可以移项，例如，由 $a+b\equiv c(\mathrm{mod}\ m)$ 可以推出 $a\equiv c-b(\mathrm{mod}\ m)$，事实上，由 $a+b\equiv c$ 和 $-b\equiv -b$ 得 $a+b-b\equiv c-b$，即 $a\equiv c-b$。此外，由 1°和 4°可见，从 $a\equiv b$ 可以推出 $ac\equiv bc$，即可以用数乘合同式的两边。由 4°，我们还可以推出下面几条性质：

5°　若 $a\equiv b$，则 $a\pm k\equiv b\pm k$；

6°　若 $a+b\equiv c$，则 $a\equiv c-b$；

7°　若 $a\equiv b$，则 $ak\equiv bk$；

8°　若 $a\equiv b$，则 $a^n\equiv b^n, n>0$；

这些都和相等的性质相同。但对于数的相等，我们还有消去律，即若 $c\neq 0$ 而 $ac=bc$，则 $a=b$。这对合同并不普遍成立，例如，虽然对于模 6，2 不合同 0，却不能从合同式

$$8\equiv 14(\mathrm{mod}\ 6)$$

的两边消去 2。但是，仍有下面几条性质成立：

9°　若 c 和 m 互质，则 $ac\equiv bc(\mathrm{mod}\ m)$ 的充要条件是 $a\equiv b(\mathrm{mod}\ m)$；

证明：充分性显然。

必要性，因为 $ac\equiv bc(\mathrm{mod}\ m)$，所以 $m|(ac-bc)$，即 $m|(a-b)c$，又因 $(m,c)=1$，由 §2，定理 1 知，

$$m|(a-b)，即\ a\equiv b(\mathrm{mod}\ m)。$$

10°　设 $c\neq 0$，则 $ac\equiv bc(\mathrm{mod}\ mc)$ 的充要条件是 $a\equiv b(\mathrm{mod}\ m)$；

证明：必要性，因为 $ac\equiv bc(\text{mod } mc)$，所以 $ac-bc=qmc$，又因 $c\neq0$，所以 $a-b=qm$，即 $a\equiv b(\text{mod } m)$。

充分性，由已知得，$a-b=mq$，所以 $ac-bc=mcq$，即 $ac\equiv bc(\text{mod } mc)$。

11° 若 $ac\equiv bc(\text{mod } m)$ 且 $(c,m)=d$，则 $a\equiv b(\text{mod } m/d)$；

证明：由已知得，$ac-bc=mq$，所以 $ac/d-bc/d=mq/d$，其中 c/d，m/d 为整数，且互质，所以 $ac/d\equiv bc/d(\text{mod } m/d)$，由 9°得 $a\equiv b(\text{mod } m/d)$。

12° 设 p 为质数，c 不合同 0 模 p，则 $ac\equiv bc(\text{mod } p)$ 当且仅当 $a\equiv b(\text{mod } p)$；

证明：充分性显然。

必要性，由已知，c 与 p 互质，所以由 9°得 $a\equiv b(\text{mod } p)$。

模 m 合同既然是一种等价关系，就可以把所有整数按照模 m 合同的关系分为等价类，每一个等价类称为模 m 的一个剩余类。同一个剩余类的数互相合同，不同的剩余类中的数不互相合同。因为，以 m 除任意整数，可能得到的余数恰有 $0,1,\cdots,m-1$，这 m 个数，所以模 m 共有 m 个剩余类，从每个类中取出一个数作为代表，这样便可得到 m 个数，比方 $r_1,\cdots,r_m$ 说是作成一个完全剩余系，任意整数模 m 恰合同于此完全剩余系中的一个数。例如，$0,1,\cdots,m-1$ 便是这样一个完全剩余系。又如，模 3，三个数 0，1，2 作成一个完全剩余系，$-1,0,1$ 也作成一个完全剩余系。模 2，两个数 0，1 作成一个完全剩余系，0 代表所有偶数，1 代表所有奇数。

定理 1 若 a 和 m 互质，b 任意，则模 m 恰有一个数 x 使

$$ax\equiv b(\text{mod } m)。$$

证明：因为 $(a,m)=1$，所以存在 s，t 使得

$$sa+tm=1$$

所以 $sab+tmb=b$，于是 $asb\equiv b(\text{mod } m)$。

设 $x=sb$，则 sb 所在的剩余类是解。

唯一性，若 $ax\equiv b(\text{mod } m)$，$ay\equiv b(\text{mod } m)$，

则 $ax-ay\equiv0(\text{mod } m)$，因为 $(a,m)=1$，所以 $x-y\equiv0(\text{mod } m)$，即 $x\equiv y(\text{mod } m)$。

推论 设 p 为质数，a 不是 p 的倍数，则 $ax\equiv b(\text{mod } p)$ 恰有一解。

定理 2 设 $(a,m)=d>1$ 且 d 不整除 b，则 $ax\equiv b(\text{mod } m)$ 无解。

证明：反证法，若有 $ax_0\equiv b(\text{mod } m)$ 存在 q，使得 $ax_0-b=qm$，所以 $d\mid b$，矛盾。

定理 3 设 $(a,m)=d>1$，且 $d\mid b$，则 $ax\equiv b(\text{mod } m)$ 有 d 个解分别如下：

$$\alpha,\alpha+m/d,\alpha+2m/d,\cdots,\alpha+(d-1)m/d$$

其中 α 是 $\frac{a}{d}x\equiv\frac{b}{d}\left(\text{mod } \frac{m}{d}\right)$ 的解。

证明：略，感兴趣的读者自己证明。

习　　题

1. 若质数 $p\geq5$，求证 $p^2\equiv1(\text{mod } 24)$。
2. 解合同式 $35x\equiv1(\text{mod } 97)$。
3. 设 p 为质数，求证 $(a+b)^p\equiv a^p+b^p(\text{mod } p)$。

提示：用二项式定理展开 $(a+b)^p$。

4. 证明 Wilson 定理：

$$(p-1)! \equiv -1 (\bmod p)$$

其中 p 为质数。提示:2,3,…,$p-2$ 各数分为一些对,每对相乘合同于 1。

5. 表演者给计算机一个命令,计算机显示一个三位数。他请观众任意写一个三位数并同显示的数相乘,然后把乘积的后三位数告诉他。他把此数输入计算机,计算机立即显示出观众原取的那个三位数!然后可以重复以上的表演:计算机显示一个新的乘数,观众取一个新数,如此等等。继续表演多次,计算机逐次显示的乘数很分散,看不出有什么规律。试编一个程序使能产生上述效果。

§4　秦九韶定理　Euler 函数

定理 1(秦九韶定理)　设 $m_1, m_2, \cdots, m_k$ 两两互质,设对每个 m_i 指定一个整数 a_i。这样,对模 $m_1 \cdots m_k$,恰有一个整数 x 存在,适合下列合同式:

$$\left.\begin{array}{c} x \equiv a_1 (\bmod m_1) \\ \cdots \\ x \equiv a_k (\bmod m_k) \end{array}\right\} \qquad (*)$$

为了求解,我们先构造一些满足局部性质的项,再把这些项合起来,满足整体。这里"局部"是指(*)式每一个合同式,即构造 y_i,使 $y_i \equiv a_i (\bmod m_i)$,而 y_i 不影响其余合同式,即 $y_i \equiv 0 (\bmod m_j), j \neq i$。

进一步只需构造 l_i,使 $\begin{cases} l_i \equiv 1 (\bmod m_i) \\ l_i \equiv 0 (\bmod m_j) \quad j \neq i \end{cases}$　(1)

令 $y_i = a_i l_i$,则 $\begin{cases} y_i \equiv a_i (\bmod m_i) \\ y_i \equiv 0 (\bmod m_j) \quad j \neq i \end{cases}$

再令 $x = \sum_{i=1}^{k} y_i$,则 x 为所求。

下面看一下 l_i 的构造,由(1)的第二式,

$$l_i \equiv (\bmod m_j), j \neq i$$

于是 $m_j\ l_i, j \neq i$。由 §2 定理 3,则 $\prod_{j\neq i} m_j | l_i$

因此 l_i 为 $q_i\left(\prod_{j\neq i} m_j\right)$ 形式,而 l_i 满足 $l_i \equiv 1 (\bmod m_i)$,因此 q_i 满足

$$q_i\left(\prod_{j\neq i} m_j\right) \equiv 1 (\bmod m_i)$$

由上节定理 1,得 q_i 存在,$q_i = bs$。

综上,我们有如下证明:

先证明对每一个 m_i 存在 l_i 使得

$\begin{cases} l_i \equiv 1 (\bmod m_i) \\ l_i \equiv 0 (\bmod m_j) \quad j \neq i \end{cases}$,由 §2 定理 $2\left(m_i, \prod_{j\neq i} m_j\right) = 1$

所以存在 S_i, T_i 使得

$$T_i m_i + S_i\left(\prod_{j\neq i} m_j\right) = 1$$

令 $l_i = S_i\left(\prod_{j\neq i} m_j\right)$,则 $l_i \equiv 1 (\bmod m_i)$

且 $l_i \equiv 0 (\bmod m_j), j \neq i$

再令 $x=a_1l_1+a_2l_2+\cdots+a_kl_k$， (2)

则 $x(\mathrm{mod}\ m_i)\equiv a_1l_1(\mathrm{mod}\ m_i)+\cdots+a_kl_k(\mathrm{mod}\ m_i)\equiv 0+\cdots+a_i+\cdots+0\equiv a_i$，

所以 x 即为所求。

下面我们来证唯一性。

设 x'，x''为（*）式的解，则

$x'\equiv a_i(\mathrm{mod}\ m_i)$，$x''\equiv a_i(\mathrm{mod}\ m_i)$，于是

$x'-x''\equiv 0(\mathrm{mod}\ m_i)$ 即 $m_i|x'-x''$。注意到 m_i 两两互质，由§2 定理 3 得 $m_1\cdots m_k|x'-x''$

所以 $x'\equiv x''(\mathrm{mod}\ m_1\cdots m_k)$。

秦九韶定理（及其推广）在数论上起着基本性的作用，上面的证明给出求 x 的一个简便的方法，这个方法（包括§1 求 S,T 的方法）秦氏称为求一术。

在(2)中，让 a_1 经过 mod m_1 的一个完全剩余系变化，…，a_k 经过 mod m_k 的一个完全剩余系变化，这样，我们共得到 $m_1\cdots m_k$ 个 x。设

$$x'=a_1'l_1+\cdots+a_k'l_k$$
$$x''=a_1''l_1+\cdots+a_k''l_k$$

是两个这样的 x，于是，

$$\left.\begin{aligned}x'&\equiv a_1'(\mathrm{mod}\ m_1)\\&\cdots\\x'&\equiv a_k'(\mathrm{mod}\ m_k)\end{aligned}\right\}$$
$$\left.\begin{aligned}x''&\equiv a_1''(\mathrm{mod}\ m_1)\\&\cdots\\x''&\equiv a_k''(\mathrm{mod}\ m_k)\end{aligned}\right\}$$

所以，若 $a_1',\cdots,a_k'$ 和 $a_1'',\cdots,a_k''$ 不完全相同，则 x' 与 x''关于模 $m_1\cdots m_k$ 不合同。

这就是说，我们得到的 $m_1\cdots m_k$ 个 x 模 $m_1\cdots m_k$ 在不同的剩余类内。但模 $m_1\cdots m_k$ 只有 $m_1\cdots m_k$ 个剩余类，所以下面的定理成立：

定理 2 设 $m=m_1\cdots m_k$，而 $m_1,\cdots,m_k$ 两两互质。在(2)中，使 $a_1,\cdots,a_k$ 分别遍历 mod m_1，…，mod m_k 的各一个完全剩余系，则 x 遍历 mod m 的一个完全剩余系。

命题 设 A 为 mod n 的一个剩余系，若 A 中有一个数与 n 互质，则 A 中任意数与 n 互质，此时称剩余类 A 与 n 互质。

证明：设 $a,b\in A$，$a=b+qn$，

从而 $(a,n)=1\Leftrightarrow(b,n)=1$。

定义 从与模 n 互质的剩余类中各取一数作成的集合称为模 n 的一个简化剩余系。

定义 与模 n 互质的剩余系个数，记为 $\varphi(n)$，称为模 n 的 Euler 函数。

显然，简化剩余系中元素数为 $\varphi(n)$，$\varphi(n)<n$，即 $\varphi(n)$是小于等于 n 的正数中与 n 互质的个数。

例如，取 $n=10$，则完全剩余系为$\{0,1,\cdots,9\}$，简化剩余系为$\{1,3,7,9\}$，$\varphi(10)=4$。

同理，$\varphi(2)=1$，$\varphi(3)=2$，$\varphi(4)=2$，$\varphi(5)=4$，…。

定理 3 设 $m=m_1\cdots m_k$，$m_1,\cdots,m_k$ 是两两互质的，则 $\varphi(m)=\varphi(m_1)\cdots\varphi(m_k)$

证明：设 E，E_1，…，E_k 为 m，m_1，…，m_k 的各自一个简化剩余系，往证 E，$E_1\times\cdots\times E_k$ 可以建立一一对应关系即可。

设 $\sigma: E_1\times\cdots\times E_k\to E$，$\sigma((a_1,\cdots,a_k))=x$，$x=a_1l_1+a_2l_2+\cdots+a_kl_k$，其中 l_i 是定理 1 中求出的，且对任意 $(a_1,\cdots,a_k)\in E_1\times\cdots\times E_k$，有 $(a_i,m_i)=1$，$i=1,\cdots,k$，因为 $x\equiv a_i(\bmod m_i)$，所以根据命题有 $(x,m_i)=1$，$i=1,\cdots,k$，于是 $(x,m_1\cdots m_k)=1$，即 $(x,m)=1$，从而 $x\in E$，所以 σ 是 $E_1\times\cdots\times E_k$ 到 E 内的一个映射。

对任意 $x\in E$，由已知有 $(x,m)=1$，所以 $(x,m_i)=1$，又由定理 2 知 σ 为单射且存在 $(a_1,\cdots,a_k)\in D_1\times\cdots\times D_k$，使得 $x\equiv a_i(\bmod m_i)$，其中 D_i 为 m_i 的一个完全剩余系，因此 $(a_i,m_i)=1$，即 $a_i\in E_i$，从而 σ 为满射，于是，σ 是 $E_1\times\cdots\times E_k\to E$ 的一一对应关系。

因为 E 中元素数为 $\varphi(m)$，E_i 中元素数为 $\varphi(m_i)$，所以

$$\varphi(m)=\varphi(m_1)\cdots\varphi(m_k)$$

定理 4 设 $m=p_1^{r_1}\cdots p_n^{r_n}$ 为 m 的质因数分解式，$p_1,\cdots,p_n$ 都不同，于是

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_n}\right)$$

证明：先求 $\varphi(p^r)$，其中 p 为质数。

因为 $0,1,\cdots,p^r-1$ 中与 p^r 不互质的数为 $0,p,2p,\cdots,(p^{r-1}-1)p$ 共有 p^{r-1} 个，

所以 $\varphi(p^r)=p^r-p^{r-1}=p^r\left(1-\frac{1}{p}\right)$，由定理 3 有

$$\begin{aligned}\varphi(m)&=\varphi(p_1^{r_1})\cdots\varphi(p_n^{r_n})\\&=p_1^{r_1}\left(1-\frac{1}{p_1}\right)\cdots p_n^{r_n}\left(1-\frac{1}{p_n}\right)\\&=m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_n}\right)\end{aligned}$$

定理 5(Fermat－Euler 定理) 若 a 和 n 互质，则

$$a^{\varphi(n)}\equiv 1(\bmod n)。$$

证明：因为 a 和 n 互质，由 $ax\equiv ay(\bmod n)$ 可以推出 $x\equiv y(\bmod n)$，而且 x 和 n 互质时，ax 也和 n 互质，取 mod n 的一个简化剩余系 $r_1,\cdots,r_{\varphi(n)}$，于是，$ar_1,\cdots,ar_{\varphi(n)}$ mod n 都不同，且都和 n 互质，因个数也是 $\varphi(n)$，可见，它们也作成 mod n 的一个简化剩余系，所以，它们应按一定次序和 $r_1,\cdots,r_{\varphi(n)}$ 合同，因此

$$ar_1\cdots ar_{\varphi(n)}\equiv r_1\cdots r_{\varphi(n)}(\bmod n)$$

所以，$a^{\varphi(n)}\equiv 1(\bmod n)$

推论(Fermat 定理) 若 p 是质数而 p 不整除 a，则 $a^{p-1}\equiv 1(\bmod p)$。

习 题

1. 今有物不知其数，三三数之剩二、五五数之剩三，七七数之剩二，问至少物几何？(孙子算经)

2. 今天是星期一，$10^{10^{10}}$ 天后是星期几？

第六章 群 与 环

§1 置 换

定义 设 M 是一个非空的有限集合，M 的一个一对一变换称为一个置换。设 M 的元素为 $a_1,a_2,\cdots,a_n$，则 M 的置换 σ 可以简记为

$$\sigma=\begin{pmatrix}a_1 & a_2 & \cdots & a_n\\ b_1 & b_2 & \cdots & b_n\end{pmatrix}\quad b_i=\sigma(a_i),i=1,2,\cdots,n.$$

因为置换按定义是一对一的，所以 $b_1,b_2,\cdots,b_n$ 是 $a_1,a_2,\cdots,a_n$ 的一个排列。由此可见，M 的每个置换对应 $a_1,a_2,\cdots,a_n$ 的一个排列，不同的置换对应不同的排列，此外，$a_1,a_2,\cdots,a_n$ 的任意排列也确定 M 的一个置换。所以，M 的置换共有 $n!$ 个，其中 n 是 M 的元数。

定义 对任意 $a\in M$，及置换 σ,τ，σ 和 τ 的乘积记为 $\sigma\tau$：

$$\sigma\tau(a)=\sigma(\tau(a))$$

容易证明，置换的乘积不满足交换律。

定义 设 σ 是 M 的置换，若可取到 M 的元素 $a_1,a_2,\cdots,a_r$ 使 $\sigma(a_1)=a_2,\sigma(a_2)=a_3,\cdots,\sigma(a_{r-1})=a_r,\sigma(a_r)=a_1$，而 σ 不变 M 的其余的元素，则 σ 称为一个轮换，记为

$$(a_1\,a_2\cdots a_r)$$

当然，也可以把 $a_1,a_2,\cdots,a_r$ 中的任意元素 a_i 排在头一位而改写成

$$(a_i\,a_{i+1}\cdots a_r\,a_1\,a_2\cdots a_{i-1})$$

定义 M 的两个轮换 $\sigma=(a_1\cdots a_n)$ 和 $\tau=(b_1\cdots b_s)$ 说是**不相杂或不相交**，如果 $a_1,\cdots,a_r$ 和 $b_1,\cdots,b_s$ 都不相同。

例如，(1 3 5)和(2 4 6)不相交；。(1 3 5)和(2 3 6)相交。

又如，
$$(1\,3\,5)(2\,4\,6)=\begin{pmatrix}1&3&5\\3&5&1\end{pmatrix}\begin{pmatrix}2&4&6\\4&6&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\3&4&5&6&1&2\end{pmatrix}=(2\,4\,6)\,(1\,3\,5)。$$

$$(1\,3\,5)(1\,4\,6)=\begin{pmatrix}1&3&5\\3&5&1\end{pmatrix}\begin{pmatrix}1&4&6\\4&6&1\end{pmatrix}=\begin{pmatrix}1&3&4&5&6\\4&5&6&1&3\end{pmatrix}=(1\,4\,6\,3\,5)。$$

下面我们来证明：若 σ 和 τ 是两个不相杂的轮换，则其乘法适合交换律，即 $\sigma\tau=\tau\sigma$

设 $\sigma=(a_1\cdots a_r)$，$\tau=(b_1\cdots b_s)$，则对 $x\in M$，不妨设 x 是 a_i 或 b_i，若 x 是某 a_i，因 τ 不变 a_j，$j=1,\cdots,r$，有

$$\sigma\tau(x)=\sigma\tau(a_i)=\sigma(a_i)=a_{i+1}$$

$$\tau\sigma(x)=\tau\sigma(a_i)=\tau(a_{i+1})=a_{i+1}$$

$i=r$ 时 a_{i+1} 应改为 a_1。

所以，$\sigma\tau(x)=\tau\sigma(x)$，若 x 是某 b_i，同理可推出此结论。

定理1　任意置换 σ 恰有一法写成不相杂的轮换乘积。

证明：先证 σ 可以写成不相杂的轮换的乘积。

取任意 $a_1\in M$，若 $\sigma(a_1)=a_1$，则 a_1 自己就作成一个轮换。

设 $\sigma(a_1)=a_2,\sigma(a_2)=a_3,\cdots$。这样下去，由于 M 有限，故到某一个元素 a_r，其 $\sigma(a_r)$ 必然不能再是新的元素，即这 $\sigma(a_r)$ 必在 $a_1,\cdots,a_r$ 之内。由于 σ 是一对一的，我们已有 $\sigma(a_i)=a_{i+1},i=1,\cdots,r-1$，所以 $\sigma(a_r)$ 只能是 a_1。于是我们得到一个轮换 $(a_1,\cdots,a_r)$。若 M 已经没有另外的元素，则 σ 就等于这个轮换。否则设 b_1 不在 $a_1,\cdots,a_r$ 之内，则同样作法又可得到一个轮换 $(b_1\cdots b_s)$。因为 $a_1,\cdots,a_r$ 各自已有变到它的元素，所以 $b_1,\cdots,b_s$ 中不会有 $a_1,\cdots,a_r$ 出现，即这两个轮换不相杂。若 M 的元素已尽，则 σ 就等于这两个轮换的乘积，否则如上又可得到一个轮换。如此类推，由于 M 有限，最后必得

$$\sigma=(a_1\cdots a_r)(b_1\cdots b_s)\cdots(c_1\cdots c_t) \tag{1}$$

即 σ 表成了不相杂的轮换的乘积。

再证表法唯一。设 σ 又可表为不相杂的轮换的乘积如下：

$$\sigma=(a'_1\cdots a'_{r'})(b'_1\cdots b'_{s'})\cdots(c'_1\cdots c'_{t'}) \tag{2}$$

试看(1)式中的任意轮换，例如 $(a_1\cdots a_r)$。a_1 必出现在(2)式中的某个轮换之内，例如 $(a'_1\cdots a'_{r'})$。由于一个轮换中任意元素都可排在头一位，不妨假定 $a_1=a'_1$。于是，

$$a_2=\sigma(a_1)=\sigma(a'_1)=a'_2,a_3=\sigma(a_2)=\sigma(a'_2)=a'_3,\cdots,$$

如此类推，可见 $(a_1\cdots a_r)$ 必和 $(a'_1\cdots a'_{r'})$ 完全相同。这就是说，(1)中的任意轮换必出现在(2)中，同样(2)中的任意轮换必出现在(1)中。因之，(1)和(2)一样，最多排列的方法不同。但不相杂的轮换相乘适合交换律，所以排列的次序本来是可以任意颠倒的。所以表法唯一。

例如，设 M 的元素为 4，于是 M 的 24 个置换可以写成下面的形式：

I；

(1 2)，(1 3)，(1 4)，(2 3)，(2 4)，(3 4)；

(1 2 3)，(1 3 2)，(1 2 4)，(1 4 2)，(1 3 4)，(1 4 3)，(2 3 4)，(2 4 3)；

(1 2 3 4)，(1 2 4 3)，(1 3 2 4)，(1 3 4 2)，(1 4 2 3)，(1 4 3 2)；

(12)(3 4)，(1 3)(2 4)，(1 4)(2 3)。

定义　设 $(a_1\cdots a_r)$ 为一轮换，称 r 为该轮换的长度。长度为 2 的轮换称为对换。

显然，一个轮换的长度也就是其中所含的元素数且任意轮换可以写成对换的乘积。

例如，$(a_1\cdots a_r)=(a_1\,a_r)(a_1\,a_{r-1})\cdots(a_1\,a_3)(a_1\,a_2)$　(3)

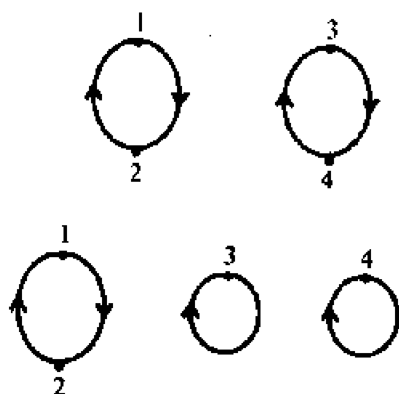
写成了 $r-1$ 个对换。

推论1　对任意置换，有一法(但未必只有一法)可将其写成一些对换的乘积。

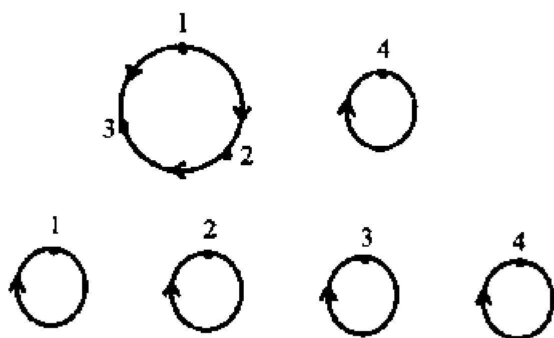
这里，乘积中出现的诸对换已非不相杂，例如上列公式中的诸对换竟一律杂以 a_1。而且，表法也不唯一，如

$$(1\ 2)=(1\ 2)(1\ 3)(1\ 3)=(2\ 3)(1\ 3)(2\ 3)$$

置换表成一组轮换之乘积后，就可以在平面上用一组顺向圈来表示。这样，就得到一个平面上的有向图形，它直观地描绘出元素之间的变换关系。例如，设 $M=\{1,2,3,4\}$，置换(1 2)(3 4)和(1 2)分别有图形



置换(1 2 3)和 I 分别有图形



图中，我们从 a 向 b 引一箭头，就表示在该置换下，a 变成 b。

这里，每个顺向圈的长度，即圈上所含的元素个数，就是该圈所表示的轮换的长度。

总之，一个 n 元置换对应一组顺向圈，这组圈的长度之总和为 n；反之，一组顺向圈表示一置换，置换的元素个数就是组中各圈长度之总和。

一组顺向圈又可以用一个式子

$$\alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_r z_r \text{(诸 } \alpha \text{ 为非负整数)}$$

来表达，其中 z_i 表示长度为 i 的圈，而 z_i 的系数 α_i 则表示如此的 z_i 的个数。例如，置换(1 2)(3 4)，(1 2)，(1 2 3)和 I，其图形可以分别表达成式子

$$2z_2, 2z_1 + z_2, z_1 + z_3 \text{和 } 4z_1\text{。}$$

总之，一个 n 元置换 σ 有一图形表达式

$$G_\sigma = \alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_r z_r$$

其中 $\alpha_1 + 2\alpha_2 + \cdots + r\alpha_r = n$ 称为该置换的图型。因为 n 元置换最多只能出现 1 个最长的圈 z_n，也最多只能出现 n 个最短的圈 z_1，所以对于上列的图形表达式 G_σ，总可写成

$$G_\sigma = \sum_{i=1}^{n} \alpha_1 z_1 + \alpha_2 z_2 + \cdots + \alpha_r z_r,$$

$$0 \le \alpha_1 \le n; \alpha_n = 0 \text{ 或 } 1$$

全部 α 都是非负整数。

设 σ 表为 k 个不相杂的轮换的乘积，这些轮换的长度分别为 $r_1, \cdots, r_k$。视 $\sum_{j=1}^{k}(r_j - 1) = n - k$，(计 k 时包括长度为 1 的轮换在内)为奇或为偶，我们说 σ 是一个奇

置换或偶置换。由前面的定理1及公式(3)，我们知道这样的 σ 可表为 $\sum_{j=1}^{k}(r_j-1)$ 个对换的乘积。于是，奇置换可表为奇数个对换之积，偶置换可表为偶数个对换之积。我们定义一个置换 σ 的符号 $\mathrm{sgn}\sigma$ 如下：

$$\mathrm{sgn}\sigma=(-1)^{\sum_{j=1}^{k}(r_j-1)}$$

即对偶置换 σ，$\mathrm{sgn}\sigma=1$，奇置换 σ，$\mathrm{sgn}\sigma=-1$。例如，若 $\sigma=(1\ 2\ 3)$，则 $\mathrm{sgn}\sigma=1$；若 $\sigma=(1\ 2)$，则 $\mathrm{sgn}\sigma=-1$。

引理　$\mathrm{sgn}\sigma\tau=\mathrm{sgn}\sigma\mathrm{sgn}\tau$

证明：首先设 $\sigma=(a\ b)$，τ 是任意置换，根据定理1，τ 分解为不相杂轮换乘积，看 $\sigma\tau=(a\ b)\tau$ 有两种情况：

A) a,b 分别在 τ 的两个不同轮换之内，不妨写成

$$\tau=(a\ a_1\cdots a_s)(b\ b_1\cdots b_t)\cdots$$

所以 $\mathrm{sgn}\tau=(-1)^{s+t+\cdots}$

不难看出 $(a\ b)\tau=(a\ a_1\cdots a_s\ b\ b_1\cdots b_t)\cdots$

即 $\mathrm{sgn}(a\ b)\tau=(-1)^{s+t+1+\cdots}$

$=(-1)\mathrm{sgn}\tau$

B) a,b 在 τ 的同一轮换内，不妨设 $\tau=(a\ a_1\cdots a_s\ b\ b_1\cdots b_t)\cdots$

则 $\mathrm{sgn}\tau=(-1)^{s+t+1+\cdots}$

又因 $(a\ b)\tau=(a\ b)(a\ a_1\cdots a_s\ b\ b_1\cdots b_t)\cdots$

$=(a\ a_1\cdots a_s)(b\ b_1\cdots b_t)\cdots$

即 $\mathrm{sgn}(a\ b)\tau=(-1)^{s+t+\cdots}$

$=(-1)\mathrm{sgn}\tau$

其次，我们来看 σ 也是任意置换，它可分解为 $\sum_{j=1}^{k}(r_j-1)$ 个对换乘积，由前面已证出的结论可知，每乘入一个对换，就使 $\mathrm{sgn}\tau$ 变换一次符号，逐次乘入 $\sum_{j=1}^{k}(r_j-1)$ 个对换，变号 $\sum_{j=1}^{k}(r_j-1)$ 次，故 $\mathrm{sgn}\sigma\tau=(-1)^{\sum_{j=1}^{k}(r_j-1)}\mathrm{sgn}\tau$。

所以引理成立。

由引理不难看出：

偶置换×偶置换＝偶置换，奇置换×奇置换＝偶置换

奇置换×偶置换＝奇置换，偶置换×奇置换＝奇置换。

定理2　每个置换都能分解为对换的乘积，但偶置换只能分解为偶数个对换的乘积，奇置换只能分解为奇数个对换的乘积。

证明：定理中的第一句断言是定理1推论1的复述。第二句断言中“能分解”之说也已说明，现在需要证明的是“只能分解”。

若不然，设偶置换分解成了奇数个对换的乘积，但对换是奇置换，奇数个奇置换乘积是奇置换，矛盾，所以偶置换只能分解为偶数个对换的乘积，同理奇置换只能分解为奇数个对换的乘积。

定理3　设 M 的元数为 n。若 $n>1$，则奇置换的个数和偶置换的个数相等，因而都等于 $n!/2$。

证明：命 $\tau_1,\cdots,\tau_m$ 是所有偶置换，τ_i 各不相同，由于 $n>1$，故可以取到一个对换 ρ，作下列乘积

$$\rho\tau_1,\cdots,\rho\tau_m$$

(1) $\rho\tau_i$ 是奇置换，显然。

(2) $\rho\tau_i\neq\rho\tau_j$ 当 $i\neq j$ 时。

若不然，则 $\rho\tau_i=\rho\tau_j$，用 ρ^{-1} 左乘得，$\tau_i=\tau_j$，矛盾！即 $\rho\tau_i\neq\rho\tau_j$。

所以，奇置换最少 m 个，即奇置换个数≥偶置换个数，再设 $\sigma_1,\cdots,\sigma_t$ 是所有奇置换，同理可推得偶置换个数≥奇置换的个数，所以结论成立。

定义 定义 σ 之奇偶性的整数 $\sum_{j=1}^{k}(r_j-1)=n-k$，称为置换 σ 的*定性数*，其中，k 是包括长度为 1 的轮换在内的轮换个数，$r_1,\cdots,r_k$ 是 k 个轮换的长度。

定理 4 设 n 元置换 σ 有图型

$$G_\sigma=\sum_{r=1}^{n}\alpha_r z_r$$

则 σ 之定性数等于

$$f_\sigma=\sum_{r=2}^{n}(r-1)\alpha_r$$

证明：因为 $n=\alpha_1+2\alpha_2+\cdots+n\alpha_n=\sum_{r=1}^{n}r\alpha_r$

$$k=\alpha_1+\alpha_2+\cdots+\alpha_n=\sum_{r=1}^{n}\alpha_r$$

$$f_\sigma=n-k=\alpha_2+\cdots+(n-1)\alpha_n=\sum_{r=2}^{n}(r-1)\alpha_r$$

换言之，视该和数 f_σ 之为奇数或偶数，σ 即为一奇置换或偶置换。

习　　题

1. 计算(1 2 3)(2 3 4)(1 4)(2 3)

2. 用 $1,2,\cdots,n$ 代表 M 中的元素，求证 M 的任意置换可以表为(1 2)，(1 3)，…，(1 n)的乘积，又可以表为(1 2)，(2 3)，…，($n-1$ n)的乘积。

3. 设 σ、τ 是两个置换，把 τ 表为不相杂的轮换的乘积，求证计算 $\sigma\tau\sigma^{-1}$ 只要用 σ 变换 τ 中的文字。例如 $\sigma=(1\ 2\ 3)$，$\tau=(1\ 2)(3\ 4)$，则 $\sigma\tau\sigma^{-1}=(2\ 3)(1\ 4)$，即按照 σ 的变法把 τ 中之 1 换成 2，2 换成 3，3 换成 1，即得 $\sigma\tau\sigma^{-1}$。

§2　群的定义

定义 设 M 是非空集合，若对任意 $x,y\in M$，都有 M 中唯一确定元素 z 与之对应，则称此对应为 M 上的一个(二元)*代数运算*。

定义 设 M 是非空集合，若 M 上定义一种代数运算(记·)，且满足结合律：$(x\cdot y)\cdot z=x\cdot(y\cdot z)$，则称$(M,\cdot)$为*半群*，有时也简称 M 是半群。

有时·在表达式中也可以省略。

定义 设 G 是半群，如果

1) G 中有一个元素 1，适合 $1a=a1=a$；

2) 对任意 $a\in G$，有 a^{-1} 适合 $aa^{-1}=a^{-1}a=1$，

则称 G 为群。

例如，(整数，+)，(有理数，+)，(实数，+)，(n 元置换集合，置换乘积)，(n 元偶置换集合，置换乘积)都是群；(整数，乘法)，(n 元奇置换集合，置换乘法)就不是群。

定理 1 设 G 是一个群，G 中恰有一个元素 1 适合 $1a=a1=a$，而且，对于任意 a 恰有一个元素 a^{-1} 适合 $aa^{-1}=a^{-1}a=1$。

证明：设又有 $1'$ 也是单位元，则 $1=11'=1'$，故群中 1 唯一。

对任 $a\in G$，设 b,c 都有 a^{-1} 的性质，则 $b=b1=b(ac)=(ba)c=1c=c$。

a^{-1} 叫 a 的逆，容易证明 $(a^{-1})^{-1}=a$。

定理 2 群定义中的条件 1)和 2)可以减弱如下：

1)′ G 中有一个左壹，$1a=a$

2)′ 对任意 a，有一个左逆 a^{-1}，$a^{-1}a=1$

证明：需要从 1)′，2)′加上结合性，封闭性，证出 1)，2)。

(先证 $aa^{-1}=1$)

对任 $a\in G$，由已知有 a^{-1}，使 $a^{-1}a=1$，考虑 $a^{-1}a\,a^{-1}=1\,a^{-1}=a^{-1}$，$a^{-1}$ 也应有左逆，设为 b，即 $b\,a^{-1}=1$

所以，$b\,a^{-1}a\,a^{-1}=b\,a^{-1}$，看此等式，

左边 $=b\,a^{-1}a\,a^{-1}=(b\,a^{-1})(a\,a^{-1})=1(a\,a^{-1})=a\,a^{-1}$，

右边 $=ba^{-1}=1$，

所以 $a\,a^{-1}=1$。

(再证 $a1=a$)

对任 $a\in G$，由已知有 1，使 $1a=a$，于是

$$a1=a(a^{-1}a)=(a\,a^{-1})a=1a=a。$$

自然，把 1)′，2)′中对于左边的要求一律改成对于右边的要求也是一样的。

定理 3 1)和 2)等价于下列可除条件：对于任意 a,b，有 x 使 $xa=b$，又有 y 使 $ay=b$。

证明：必要性，显然，只要取 $x=b\,a^{-1}$，$y=a^{-1}b$ 即可。

充分性，只需证明根据可除条件能推出 1)′，2)′即可。

任意取定 $c\in G$，看 $xc=c$，由已知它有解，记解为 1_c，于是 $1_c c=c$，

先证 1)′ 往证对任意 $a\in G$，$1_c a=a$。

对任意 a，$cy=a$ 有解，记为 y'，即 $cy'=a$，于是 $1_c a=1_c(cy')=(1_c c)y'=cy'=a$，所以 1)′式成立。

不妨将 1_c 记为 1。

再证 2)′，对于任意 a，则 $xa=1$ 有解，令这个解为 a^{-1}，则 $a^{-1}a=1$。

定理 4 设 G 是一个群，在一个乘积 $a_1\cdots a_n$ 中可以任意加括号而求其值。

证明：只要证明任意加括号而得的积等于按左至右加括号所得的积

$$(\cdots((a_1a_2)a_3)\cdots a_{n-1})a_n$$

对 n 用归纳法，当 $n=1,2$ 时，显然；

当 $n=3$ 时是结合律，假设对少于 n 个因子的乘积成立，

往证对 n 个也成立。

设任意加括号得积 A，最后一次相乘的前后二部分为 B 与 C：

$$A=(B)(C)$$

其中 B 和 C 中的因子个数均小于 n，所以 C 等于按次序自左而右加括号所得的乘积 $(D)a_n$，由结合律得，$A=(B)(C)=(B)((D)a_n)=((B)(D))a_n$，注意到 $(B)(D)$ 的因子个数小于 n，故

$$(B)(D)=(\cdots((a_1a_2)a_3)\cdots a_{n-2})a_{n-1}$$

所以 $A=((B)(D))a_n=((\cdots((a_1a_2)a_3)\cdots a_{n-2})a_{n-1})a_n$。

当给出二元运算后，若无结合律，则三个以上元素的运算不一定有意义，本定理对有结合律的一切代数体系成立。

现在 $a_1\cdots a_n$ 有意义，当它们都相同时称 n 个 a 连乘积为 a 的 n 次方，记为 a^n，再规定

$$a^0=1,a^{-n}=(a^{-1})^n,$$

于是，有第一指数律，$a^ma^n=a^{m+n}$；第二指数律，$(a^m)^n=a^{mn}$。

定义 若群 G 中乘法有交换律 $ab=ba$，则 G 叫做 Abel *群或交换群*。

定理 5 在一个交换群 G 中，一个乘积可以任意颠倒因子的次序而求其值。

证明：对积 $a_1\cdots a_n$，设 r 是 $1,\cdots,n$ 上一个置换，要证

$$a_{r(1)}a_{r(2)}\cdots a_{r(n)}=a_1a_2\cdots a_n$$

对 n 用归纳法，$n=1$ 显然，$n=2$ 是交换律。

设 $n-1$ 已对，看 n 时，记 $P=a_{r(1)}a_{r(2)}\cdots a_{r(n)}$ 其中必出现 a_n，于是可写

$$P=(P')a_n(P'')=P'(a_n(p''))=P'((P'')a_n)=P'P''a_n$$

而 $P'P''=a_1\cdots a_{n-1}$，所以 $P=a_1\cdots a_n$。定理得证。

其实，由前节习题 2，$1,\cdots,n$ 的任意置换可以表为对换 $(1\ 2),(2\ 3),\cdots,(n-1\ n)$ 的乘积。所以要证任意颠倒乘积的因子次序不变乘积的值，只要证明：颠倒乘积中相邻的两个因子的次序不变乘积的值，但这正是交换律。

在交换群中，易见有第三指数律：$(ab)^m=a^mb^m$ 成立。交换群常称为加法群，其中运算称为加法，记为"+"，于是

交换律：$a+b=b+a$

结合律：$(a+b)+c=a+(b+c)$

单位元 0：$a+0=0+a=a$

逆元称为负元 $-a$：$a+(-a)=(-a)+a=0$

在乘法群中的 a^n 现在为 $na=a+\cdots+a$

规定 $0a=0,(-n)a=-na$ 二个指数律变为：$(m+n)a=ma+na$；$m(a+b)=ma+mb$；$m(na)=(mn)a$。

习　　题

1. 试证明 n 个元素的所有置换作成一个群（通常叫做 n 次对称群）。并证明 n 个元素的所有偶置换作成一个群（叫做 n 次交代群），写出四次交代群中的元素，n 次交代群的元数为多少？

2. 举例说明不要求可除条件而要求消去条件，即要求由 $ax=ay$ 可推出 $x=y$，由 $xa=ya$

可推出 $x=y$,则 G 不见得是一个群。若 G 有限怎么样?

3. 举例说明定理 2 中的 1)′和 2)′分别改成:1)′ G 中有一个元素 1 适合 $1a=a$,2)′对于任意 a 有一个 a^{-1}适合 $aa^{-1}=1$,则 G 不见得是一个群。

4. 设 G 为群,如果 G 中任一元素 a,都有 $a^{-1}=a$,则 G 为交换群。

§3 子群及其陪集

定义 设 G 是一个群,H 是 G 的一个子集,如果按照 G 中的乘法,H 是一个群,则 H 叫做 G 的子群。

例如,群 G 是它自己的子群,{1}也是 G 的一个子群;非零有理数乘法是非零实数乘法群子群,又是非零复数乘法群的子群。

又如,三次对称群 $S_3=\{I,(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$

三次交代群 $A_3=\{I,(1\ 2\ 3),(1\ 3\ 2)\}$

则 A_3 是 S_3 的子群。

定理 1 群 G 的一个子集 H 是 G 的一个子群,必要而且只要

(1) 若 $a\in H,b\in H$,则 $ab\in H$;

(2) 若 $a\in H$,则 $a^{-1}\in H$;

(3) H 非空。

证明:必要性,设 H 是 G 的子群,则 H 是群,所以 H 中乘法满足封闭性,所以(1)式成立,同样(3)式也成立。以下证(2)。我们先证 G 中的 1 就是 H 中的 1。

假设 H 中的单位元是 $1'$,则对任意 $a\in H$,有 $1'a=a$。此式在 H 中成立,则在 G 中也必然成立,所以用 a^{-1}右乘上式得 $1'aa^{-1}=aa^{-1}$,即 $1'=1$,所以 G 中的 1 也是 H 中的单位元。

因为 H 为群,所以对任意 $a\in H$,应有 $b\in H$,使 $ab=1$,此式在 G 中也成立,用 a^{-1}左乘得 $b=a^{-1}$,所以 $a^{-1}\in H$,即(2)成立。

充分性,只需证 H 为群即可。

由(3),H 非空,由(1)封闭性成立,设 a,b,c 是 H 的任意三个元素,在 G 中有$(ab)c=a(bc)$,因 H 封闭,所以在 H 中也成立,于是 H 首先为半群。

下面证 H 中有壹,取任意 $a\in H$,由(2),$a^{-1}\in H$,由(1),$aa^{-1}\in H$,即 $1\in H$,在 G 中有 $1a=a$ 成立,在 H 中此式自然成立。

再证 H 中有逆,取 H 中任一元素 a,则有 G 中 a 的逆 $a^{-1}\in H$,在 G 中有 $a^{-1}a=1$ 成立,此式在 H 中也成立,所以按照 G 中的乘法,H 是一个群,所以 H 是 G 的子群。

定理 2 定理 1 中的两个条件(1),(2)可以换成下面一个条件:

(*) 若 $a\in H,b\in H$,则 $ab^{-1}\in H$。

证明:必要性,设 $a\in H,b\in H$,由(2) $b^{-1}\in H$,再由(1)$ab^{-1}\in H$,所以(*)式成立。

充分性,设 $a\in H$,由(*)式 $aa^{-1}\in H$,即 $1\in H$,再由(*)式得,$1a^{-1}\in H$,即 $a^{-1}\in H$,所以(2)成立。

设 $a\in H,b\in H$,所以 $b^{-1}\in H$,再由(*)式得 $a(b^{-1})^{-1}\in H$,即 $ab\in H$,故(1)成立。

定理 3 设 a 是群 G 的一个元素,于是 a 的所有幂的集合

$$a^n, n=0,\pm 1,\pm 2,\cdots$$

做成 G 的一个子群，记为 (a)，此群称为由 a 生成的子群。a 就称为 (a) 的一个生成元。

证明：首先 (a) 非空，因为 $a^0=1\in(a)$。

任取 (a) 中二元素 a^m,a^n，有 $a^m(a^n)^{-1}=a^m a^{-n}=a^{m-n}\in(a)$，故由定理 2，$(a)$ 做成了 G 的一个子群。

定义 若群 G 能由某一个元素生成，则 G 称为*循环群*或*巡回群*。

例如，$\{1,-1,i,-i\}$，将 i 记为 a，可写成 $\{a^0,a^1,a^2,a^3\}$。

又如，整数加群，1 是生成元。

定义 对群中任意元 a，考察 $\cdots,a^{-2},a^{-1},a^0,a^1,a^2,\cdots$。

情况 1，其中元素皆不同，则说 a 周期是无穷大或 0。

情况 2，其中元素有相同的，即有整数 $s\neq t$ 使 $a^s=a^t$。不妨设 $s>t$，于是 $s-t>0$ 而 $a^{s-t}=1$，即有正整数 m 使 $a^m=1$，若 n 为适合 $a^n=1$ 的最小正整数，则说 a 的周期为 n。

例如，在所有非 0 复数构成的乘法群中，1 的周期为 1，-1 的周期为 2，$\pm i$ 的周期为 4，模数 $r\neq1$ 的复数 $z=re^{i\theta}$ 的周期为无穷大。

定理 4 若群 G 中元素 a 的周期为 n，则

(1) $1,a,a^2,a^3,\cdots,a^{n-1}$ 为 n 个不同元素；

(2) $a^m=1$ 当且仅当 $n\mid m$；

(3) $a^s=a^t$ 当且仅当 $n\mid(s-t)$

证明：先证(2)，对于任意整数 m，有 $m=nq+r$，$0\leq r<n$，所以 $a^m=a^{nq}a^r=(a^n)^q a^r=1^q a^r=a^r$，由于 n 是使 $a^n=1$ 的最小正数，而 $r<n$，所以 $a^r=1$ 当且仅当 $r=0$，所以 $a^m=1$ 当且仅当 $a^r=1$ 当且仅当 $r=0$ 当且仅当 $n\mid m$，(2)得证，由(2)知 $a^s=a^t$ 当且仅当 $a^{s-t}=1$ 当且仅当 $n\mid(s-t)$，(3)得证，由(3)容易看出(1)是成立的。

由本定理，设 a 为群 G 的一个元素，如果 a 的周期为无穷大，则 a 生成的子群 (a) 是无限循环群，(a) 由彼此不同的元素

$$\cdots,a^{-2},a^{-1},1,a,a^2,\cdots$$

组成；如果 a 的周期为 n，则子群 (a) 为 n 元循环群，它由 n 个不同的元素

$$1,a,a^2,a^3,\cdots,a^{n-1}$$

组成。

如果群 G 是加法群，定理 4 就变为

(1′) $0,a,2a,\cdots,(n-1)a$ 为 n 个不同元素；

(2′) $ma=0$ 当且仅当 $n\mid m$；

(3′) $sa=ta$ 当且仅当 $n\mid(s-t)$

这时子群 (a) 为 n 元循环加法群，它由 n 个不同元素

$$0,a,2a,\cdots,(n-1)a$$

组成；若 a 的周期为无穷大，则子群 (a) 为无限循环加法群，它由 $\cdots,-2a,-a,0,a,2a,\cdots$ 组成。

例如，$z^n-1=0$ 在复数域中恰有 n 个不同的根

$$z_k=e^{\frac{2k\pi i}{n}},k=0,1,\cdots,n-1,$$

称为 n 次单位根，它们做成一 n 元的乘法交换群 U_n。这 U_n 可由任意一个本原 n 次单位根（即周期为 n 者）生成，例如可由 $z_1=e^{\frac{2\pi i}{n}}$ 生成。当 $n>2$ 时，本原 n 次单位根不只一个，只要 k 与

n 互质，$z_k=e^{\frac{2k\pi i}{n}}$ 便是一个本原 n 次单位根。故循环群的生成元素未必唯一。

定理 5　若 a 的周期为 n，则(a)具有 $\varphi(n)$ 个生成元素。

证明：看(a)中的元素 $1,a,a^2,\cdots,a^{n-1}$，若(a)中的某元素 b 也是生成元，则$(a)=(b)$。因 a 是生成元，可设 $b=a^k$，$0\leq k<n$，看哪些 k 使 a 可表为 b 的若干次方。设 $a=(a^k)^h$，则 $a=a^{kh}$，由定理 4 知，$n\mid(kh-1)$，所以 $kh-1=qn$，即 $kh-qn=1$，即 k 与 n 互质，反之，若 k 与 n 互质，不难证明，a 可表为 b 的若干次方。所以，a 可表为 $b=a^k$ 的若干次方，当且仅当 k 与 n 互质，但在 $0\leq k<n$ 中，共有 $\varphi(n)$ 个 k 与 n 互质，所以共有 $\varphi(n)$ 个元素生成(a)。

定义　设 H 是群 G 的一个子群，$a,b\in G$，如果

$$a=bh,h\in H,$$

则说 a 合同于 b(右模 H)，记为 $a\equiv b$(右 mod H)。

例如，$G=\{I,(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),1\ 3\ 2)\}$

$H=\{I,(1\ 2)\}$

则说$(1\ 2\ 3)$合同于$(1\ 3)$右模 H，因为$(1\ 2\ 3)=(1\ 3)(1\ 2)$，其中$(1\ 2)\in H$。

下面我们来证明合同关系是等价关系。

1)反身性：因为 $a=a1$，$1\in H$，所以 $a\equiv a$。

2)对称性：若 $a\equiv b$，则 $a=bh$，$h\in H$，所以 $b=ah^{-1}$，因为 H 是群，所以 $h^{-1}\in H$，所以 $b\equiv a$。

3)传递性：若 $a\equiv b$，$b\equiv c$，则 $a=bh$，$b=ck$，其中 $h,k\in H$，即 $a=ckh$，而 $kh\in H$，所以 $a\equiv c$。

既然合同关系(右模 H)是一个等价关系，所以 G 分成了所有等价类的并集。每一个这样的等价类叫做 H 的一个*右陪集*。

根据右陪集的定义有下面的结论：

(1) 以 H 的所有元素右乘 G 中某元素 a，所得集合记为 aH，则包含 a 的右陪集就是 aH。

证明：记包含 a 的右陪集为 B，往证 $aH=B$。

对任意 $b\in B$，因为 $a\in B$，按等价类的定义，$b\equiv a$(右 mod H)，故有 $h\in H$，使得 $b=ah$，所以 $b\in aH$，即 $B\subseteq aH$。

任取 aH 中一元素 a'，则 $a'=ah$，其中 $h\in H$，故 $a'\equiv a$(右 mod H)，a'在 a 所在的右陪集 B 中，即 $a'\in B$，所以 $aH\subseteq B$。

综上所述，$aH=b$。

(2) H 本身也是 H 的一个右陪集。

(3)包含 1 的右陪集即 H，而任何 H 外右陪集不含 1，故除 H，其它的右陪集都不是群。

同理可定义左陪集。

例如，设 G 是所有整数的加法群，H 是 m 的所有倍数作成的子群。因为加法适合交换律，所以左右之分不存在，因而，(左 mod H)和(右 mod H)是一样的，而左右陪集也是一样的。易见 $a\equiv b$(mod H)等于说 $a\equiv b$(mod m)，而 H 的陪集就是模 m 的剩余类。

又如，设 G 是所有非 0 复数的乘法群，所有其 $|z|=1$ 的复数 $z=e^{i\theta}$作成 G 的一个子群 H。$a\equiv b$(mod H)等于说 $|a|=|b|$。在复平面上，H 相当单位元，H 的所有陪集相当以原点为圆心的所有同心圆。

若 G 是一个有限群，可如下求 H 的右陪集：

(1) H 本身是一个，令 $G_i=H$，$i=0$；

(2) $i=i+1$，若 $G=G_i$，则停止；否则

任取不属于 G_i 的一个元素 a，而求 aH，令 $G_{i+1}=G_i\cup aH$，重复执行本步骤。

因为 G 有限，此过程必然停止，最后 $G=H\cup aH\cup\cdots$。

同理左陪集有相应的过程。

例如，$G=\{I,(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$

$H=\{I,(1\ 2)\}$

右陪集	左陪集
$H=\{I,(1\ 2)\}$	$H=\{I,(1\ 2)\}$
$(1\ 3)H=\{(1\ 3),(1\ 2\ 3)\}$	$H(1\ 3)=\{(1\ 3),(1\ 3\ 2)\}$
$(2\ 3)H=\{(2\ 3),(1\ 3\ 2)\}$	$H(2\ 3)=\{(2\ 3),(1\ 2\ 3)\}$

此时左陪集和右陪集不都相同。

若取 $H=\{I,(1\ 2\ 3),(1\ 3\ 2)\}$

右陪集	左陪集
$H=\{I,(1\ 2\ 3),(1\ 3\ 2)\}$	$H=\{I,(1\ 2\ 3),(1\ 3\ 2)\}$
$(1\ 2)H=\{(2\ 3),(1\ 3),(1\ 2)\}$	$H(1\ 2)=\{(1\ 3),(1\ 2),(2\ 3)\}$

这时左陪集和右陪集一样。

定义 设 G 是群，H 是 G 的子群，对任意 $g\in G$，若 $gH=Hg$，或者，H 的左右陪集没有区别，则称 H 为 G 的**正规子群**。

不难证明，交换群的所有子群都是正规子群；平凡子群 $H=\{1\}$ 和 G 也是正规子群。

命题 H 是 G 的正规子群当且仅当对任意 $g\in G$，$gHg^{-1}\subseteq H$。

证明 必要性，因为 H 是 G 的正规子群，所以对任意 $g\in G$，$gH=Hg$，所以 $gHg^{-1}\subseteq H$。

充分性，对任意 $g\in G$，则 $g^{-1}\in G$，由已知，$(g^{-1})H(g^{-1})^{-1}=g^{-1}Hg\subseteq H$，用 g 左乘此式，同时用 g^{-1} 右乘此式，得 $H\subseteq gHg^{-1}$，所以 $H=gHg^{-1}$，所以 H 是 G 的正规子群。

例如，设G：行列式不为 0 的所有 2×2 矩阵乘法群；

H：行列式值为 1 的所有 2×2 矩阵乘法群；

H'：所有$\begin{pmatrix}a&0\\0&b\end{pmatrix}$形矩阵乘法，$a$，$b$ 都不为 0。

(1) H 是 G 的正规子群

证明：对任意 $A\in G$，$B\in H$，

则 $|ABA^{-1}|=|A||B||A|^{-1}=|B|=1$，即 $ABA^{-1}\subseteq H$，所以 H 是正规子群。

(2) H'不是 G 的正规子群

例如，$\begin{pmatrix}1&0\\0&-1\end{pmatrix}\in H'$，$\begin{pmatrix}1&1\\0&1\end{pmatrix}\in G$，

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}^{-1}=\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}1&-1\\0&1\end{pmatrix}=\begin{pmatrix}1&-1\\0&-1\end{pmatrix}\begin{pmatrix}1&-1\\0&1\end{pmatrix}=$$

$\begin{pmatrix}1&-2\\0&-1\end{pmatrix}$不是 H'中元素，所以 H'不是正规子群。

定理 6 设 H 是群 G 的有限子群，则 H 的任意右陪集 aH 的元数皆等于 H 的元数。

证明：$aH=\{ah\mid h\in H\}$，因为 G 中有消去律：即由 $ax=ay$ 可得 $x=y$，故 H 中不同元素以 a 左乘后皆不同，令 H 中元素 h 与 aH 中元素 ah 对应，此对应便是一一对应映射，故 aH 与 H 中元素数相同。

同理可证，任意左陪集 Ha 中元素个数也等于 H 中元素个数。

Lagrange 定理 设 G 为有限群，则 G 的任意子群 H 的元数整除群 G 的元数。

证明：设 G,H 的元数为 m，r，对 H 看 G 的所有 s 个右陪集，则 G 恰为这 s 个右陪集之并，且不同右陪集之间无公共元素，又根据定理 6，每一陪集元数都与 H 元数相同，都等于 r，一共是 s 个右陪集，故所有右陪集的并集有元素 rs，它等于 G 的元数 m，即 $m=rs$，所以本定理成立。

定义 有限群 G 的元数除以 H 的元数所得的商，记为 $(G:H)$，叫做 H 在 G 中的**指数**。H 的指数也就是 H 的右（左）陪集的个数。从每个右陪集中选出一个元素为代表，全体代表的集合叫做一个*右代表系*或*右代表团*。设 G 有限而 $g_1,\cdots,g_s$ 作成一个右代表系，则 g_1H、$\cdots$，g_sH 便是 H 的所有右陪集而

$$G = g_1H \cup \cdots \cup g_sH$$

例如，若 G 为 n 元循环群，m 为 n 的一个正因数，则 G 有 m 元子群。

证明：设 $n=mq$，$G=(a)=\{1,a,\cdots,a^q,\cdots,a^{n-1}\}$，因为 $(a^q)^m=a^{qm}=a^n=1$，而对任意 $1\leq k<m$，这时，$1<q<n$，a 的周期为 n，故 $(a^q)^k=a^{qk}\neq 1$，所以 a^q 的周期为 m，从而 a^q 生成的子群 (a^q) 是 m 元的，得证。

定理 7 设 G 为有限群，元数为 n，对任意 $a\in G$，有 $a_n=1$。

证明：因为 G 有限，a 的周期必有限，否则 a 所生成的循环群 (a) 将无限，G 的元素将无穷多。兹命 a 的周期为 m，即 $a^m=1$，则 a 生成一个 m 元循环子群 $(a)\subseteq G$，按 Lagrange 定理，子群 (a) 的元数 $m\mid n$，即 $n=mq$，所以 $a^n=(a^m)^q=1$。

习 题

1. 令 I，(1 2)(3 4)，(1 3)(2 4)，(1 4)(2 3) 四个置换作成一个群叫 Klein 四元群。求证 Klein 四元群是四次对称群的正规子群。提示：利用 §1 习题 3。

2. 写出三次对称群的所有子群。

3. 若 H 在 G 中的右陪集的个数有限，求证左陪集的个数也有限而且和右陪集的个数相等。自然其个数也可以叫做 H 在 G 中的指数。提示：证明若 $g_1,\cdots,g_s$ 作成一个右代表系，则 $g_1^{-1},\cdots,g_s^{-1}$ 作成一个左代表系。

4. 求证若 H 在 G 中的指数等于 2，则 H 必然是 G 的正规子群。

5. 求证 G 的任意多个子群的交集仍是 G 的子群，并且，G 的任意多个正规子群的交集仍是 G 的正规子群。

6. 设 H 是 G 的子群，N 是 G 的正规子群，命 HN 为 H 的元素乘 N 的元素所得的所有元素的集合，求证 HN 是 G 的子群。

7. 设 H 是群 G 的一个有限非空子集，求证只要 H 中任意两个元素的积仍在 H 内，则 H 是 G 的子群。

8. 求证循环群的子群仍是循环群。

9. 设 G 是一个 n 元循环群，a 是一个生成元素。若 r 和 n 的最大公约数为 d，问 a^r 的周期等于什么？由此看来，G 中有多少个元素可以作为生成元素？

10. 求证若 G 的元素是一个质数，则 G 必是循环群。

§4 同态及同构

定义 把集合 A 及其上的二元代数运算·作为整体来看时，称为一个代数体系，记作 $(A,\cdot)$，当这个代数运算称为乘法时，叫做一个乘法系统。

定义 设 $(A,\cdot)$ 与 $(A',\cdot')$ 是两个代数体系，σ 是 A 到 A' 的映射，使得 $\sigma(a\cdot b)=\sigma(a)\cdot'\sigma(b)$，其中 $a,b\in A$，$\sigma(a),\sigma(b)\in A'$，· 是 A 上的运算，·' 是 A' 上的运算，则称 σ 是 A 到 A' 内的同态映射，说 A 与 $\sigma(A)$ 是同态，记为 $A\sim\sigma(A)$，若 σ 又是一一对应，则称是 A 到 A' 的同构映射，说 A 与 A' 同构，记为 $A\cong A'$。为了简便，常写成 $\sigma(ab)=\sigma(a)\sigma(b)$。显然，同构必是同态，同态不一定是同构。

例如，$(R^{+},*)$：集合指全体正整数，运算指乘法，

$(R,+)$：集合指全体实数，运算指加法，

映射 σ 是：x——$\log_a x$ （$a>0$ 的实数）

不难说明 σ 是一一对应。

σ 是同构映射，因为 $\sigma(x*y)=\log_a x*y=\log_a x+\log_a y=\sigma(x)+\sigma(y)$ 且是一一对应。

又例，$(C,+)$：集合是全体复数，运算是加法，

$(R,+)$：集合是全体实数，运算是加法，

令 σ： $a+b_i$——a

则 $\sigma((a+bi)+(c+di))=\sigma((a+c)+(b+d)i)=a+c=\sigma(a+bi)+\sigma(c+di)$

所以 σ 是 C 到 R 内的同态映射。

定理 1 设 G 是一个群，K 是一个乘法系统，σ 是 G 到 K 中的一个同态映射，则 G 的映象 $G'=\sigma(G)$ 是一个群。G 的壹 1 的映象 $\sigma(1)$ 就是 G' 的壹 $1'$，而 a 的逆 a^{-1} 的映象 $\sigma(a^{-1})$ 就是 a 的映象 $\sigma(a)$ 的逆：$\sigma(a^{-1})=\sigma(a)^{-1}$。

证明：1)因 G 非空，所以 G' 非空。

2)封闭性：即证若 $a'\in G'$，$b'\in G'$，则 $a'b'\in G'$。

因为必有 $a,b\in G$，使 $\sigma(a)=a'$，$\sigma(b)=b'$，由 σ 的同态性得，$\sigma(ab)=\sigma(a)\sigma(b)=a'b'$，这说明 $a'b'$ 是 G 中元素 ab 的象，故 $a'b'\in G'$。

3) 结合律：设 $a',b',c'\in G'$，要证 $a'(b'c')=(a'b')c'$。

因为 $a'=\sigma(a)$，$b'=\sigma(b)$，$c'=\sigma(c)$，而 G 中有结合律，即 $a(bc)=(ab)c$，两边作用 σ、$\sigma(a(bc))=\sigma((ab)c)$，而

$\sigma(a(bc))=\sigma(a)\sigma(bc)=a'(\sigma(b)\sigma(c))=a'(b'c')$，

$\sigma((ab)c)=\sigma(ab)\sigma(c)=(\sigma(a)\sigma(b))c'=(a'b')c'$，所以结合律成立。

4) 有左壹，并且就是 $\sigma(1)$，即对任意 $a'\in G'$，要证 $\sigma(1)a'=a'$

因 $a'=\sigma(a)=\sigma(1a)=\sigma(1)\sigma(a)=\sigma(1)a'$，所以 $\sigma(1)$ 就是 G' 中的左壹 $1'$

5) 有左逆，并且就是 $\sigma(a^{-1})$。

因为，$\sigma(a^{-1})a'=\sigma(a^{-1})\sigma(a)=\sigma(a^{-1}a)=\sigma(1)=1'$，即有左逆。

根据§2 定理 3，结论成立。

同构的群或代数系统，抽象地来看可以说毫无差别，如果 G 只和 G' 同构，则由于 G 中两个或多个元素可能变成 G' 的一个元素，所以不能说是 G 和 G' 构造一样，但因为 G 中的乘法关系在 G' 中仍对应地成立，所以，可以说 G' 是 G 的一个缩影。对 G 的缩影的研究，当然是对 G 进行

研究的重要内容或重要方法。

定义　设 σ 是 G 到 G' 上的一个同态映射，命 N 为 G 中所有变成 G' 中 $1'$ 的元素 g 的集合，记为 $\sigma^{-1}(1')$，即

$$N = \sigma^{-1}(1') = \{g \in G \mid \sigma(g) = 1'\}$$

我们把 N 叫做 σ 的核。

这里 $\sigma^{-1}(1')$ 只是一个记号，不代表逆映射。

定理 2　设 σ 是 G 到 G' 上的一个同态映射，于是，σ 的核 N 是 G 的一个正规子群，对于 G' 的任意元素 a'，$\sigma^{-1}(a')$ 是 N 在 G 中的一个陪集，因此，G' 的元素和 N 在 G 中的陪集一一对应。

证明：先证 N 是 G 的子群。

1）因为 $\sigma(1)=1'$，所以 $1\in N$，得 N 非空。

2）若 $a\in N$，则 $1'=\sigma(aa^{-1})=\sigma(a)\sigma(a^{-1})=1'\sigma(a^{-1})=\sigma(a^{-1})$，所以 $a^{-1}\in N$。

3）若 $a\in N,b\in N$，则 $\sigma(a)=1',\sigma(b)=1'$

所以 $\sigma(ab)=\sigma(a)\sigma(b)=1'1'=1'$，所以 $ab\in N$。

再证 N 是正规子群，只需证对任意 $g\in G,gNg^{-1}\subseteq N$。

因 $\sigma(gNg^{-1})=\sigma(g)\sigma(N)\sigma(g^{-1})=\sigma(g)1'\sigma(g)^{-1}=\sigma(g)\sigma(g)^{-1}=1'$，所以 $gNg^{-1}\subseteq N$。

最后证明，对任意 $a'\in G'$，而 $\sigma(a)=a'$，则 $\sigma^{-1}(a')$ 是 N 在 G 中的一个陪集，即为 aN。

因为 $\sigma(aN)=\sigma(a)\sigma(N)=\sigma(a)1'=a'$，所以 $aN\subseteq\sigma^{-1}(a')$。

对任意 $b\in\sigma^{-1}(a')$，则 $\sigma(b)=a'$，故 $(a')^{-1}\sigma(b)=1'$，$\sigma(a)^{-1}\sigma(b)=1'$，所以 $\sigma(a^{-1}b)=1'$，所以 $a^{-1}b\in N,b\in aN$，

即 $\sigma^{-1}(a')\subseteq aN$。所以 $aN=\sigma^{-1}(a')$。

容易证明：同态核是单位元群的同态必是同构。请读者自己证明。

以上说明了：若 σ 是 G 到 G' 上的同态映射，则其核 N 为一正规子群。反过来，我们要问：设 N 是 G 的一个正规子群，是否有一个群 G' 以及一个 G 到 G' 上的同态映射 σ，使 N 为 σ 的核？回答是肯定的。

引理　设 N 是 G 的正规子群。若 A,B 是 N 的陪集，则 AB 也是 N 的陪集。

证明：（群子集 A 与 B 之积 AB 规定如下：$AB=\{xy \mid x\in A,y\in B\}$）因为 N 是正规子群。故 $Nb=bN$。今设 $A=aN,B=bN$，则 $AB=aNbN=abNN=abN$，所以 AB 是一个陪集。

定理 3　按照陪集的乘法，N 的所有陪集作成一个群 $\bar{G}$。命

$$\sigma: a \to aN$$

则 σ 是 G 到 $\bar{G}$ 上的一个同态映射，其核为 N。此同态称为自然同态。

证明：由引理，$\bar{G}$ 中乘法封闭，所以 $\bar{G}$ 是乘法系统。映射 σ 使 $\sigma(a)\sigma(b)=aNbN=abN=\sigma(ab)$，故 σ 是 G 到 $\bar{G}$ 上的一个同态映射。按定理 1，$\bar{G}$ 是一个群。$\bar{G}$ 的壹显然就是 N 本身（作为 $\bar{G}$ 中的一个元素）。所以 σ 的核应含 G 中在 σ 之下变成 G 中壹 N 的那些元素：核 $\sigma=\{g \mid \sigma(g)=N\in\bar{G}\}=\{g \mid gN=N\}=\{g \mid g\in N\}=N$，所以，$N$ 是 σ 的核。

定义　若 G 为群，N 是其正规子群，则 N 的所有陪集形成的群，称为 G 对于 N 的商群，记为 G/N。

定理 4　设 σ 是 G 到 G' 上的一个同态映射，若 σ 的核为 N，则

$$G' \cong G/N$$

证明：由定理 2 知，G' 元素跟 G/H 的元素一一对应，在此对应下，对任意 $g\in G$，$\sigma(g)=g'$

时有 $g'\leftrightarrow gH$，任取 $a',b'\in G'$，$a'\leftrightarrow aN$，$b'\leftrightarrow bN$，$a'=\sigma(a)$，$b'=\sigma(b)$，而 σ 是同态映射，所以 $a'b'=\sigma(a)\sigma(b)=\sigma(ab)$，因此 $a'b'$ 对应的是 abN，这表明 $a'b'\leftrightarrow aNbN$，所以 G' 和 G/N 同构。

定理 3 和定理 4 说明，G 的任意缩影和 G 的一个商群同构，而且 G 的任意一商群也就是一个缩影。因此，抽象地看来，商群就是缩影，缩影就是商群。说是商群，我们指的是以陪集为元素作成的群。说是缩影，我们可以设想把陪集 aN 中的所有元素加以"等置"而得一个元素 a'，缩影就是这些元素 a' 作成的群。

例如，S_n：n 次对称群，$C_2=\{1,-1\}$，按照乘法，是二元循环群，规定映射 sgn：$\sigma\to\mathrm{sgn}\sigma$

则由 $\mathrm{sgn}\sigma\tau=\mathrm{sgn}\sigma.\ \mathrm{sgn}\tau$，知 sgn 是同态映射，同态象 C_2，其核为 n 次交代群 A_n，显然 A_n 是 S_n 的正规子群，$S_n\sim S_n/A_n$ 是自然同态，同态象 $C_2\cong S_n/A_n$，所以说 S_n/A_n 是二元循环群。

又如，设 I 为所有整数的加群，mI 为 m 的所有倍数作成的子群。于是 mI 的陪集就是模 m 的剩余类。由定理 3，这些剩余类按照加法作成一个群就是 I 对于 mI 的商群 I/mI。这个商群 I/mI 有 m 个元素

$$mI, 1+mI, \cdots, (m-1)+mI。$$

$1+mI$ 显然是一个生成元素，所以这个商群是一个 m 元(加法)循环群。

下面看同态映射下子群的变化。设 G 是群，同态映射 σ，$G\sim G'$，N 是同态核。

(1) H 是 G 的子群，则 $H'=\sigma(H)$ 是 G' 的子群。

(2) 设 H' 是 G' 的子群，则 $\sigma^{-1}(H')=H$ 为 G 的子群。

证明：$H=\sigma^{-1}(H')$ 显然非空。

对任意 $a,b\in H$，必有 $\sigma(a),\sigma(b)\in H'$，因 H' 是子群，所以 $\sigma(a)\sigma(b)^{-1}=\sigma(ab^{-1})\in H'$，所以 $ab^{-1}\in H$，故 H 是 G 的子群。

(3) 先给出 G 的子群 H，作 $\sigma(H)=H'$，然后看 $\sigma^{-1}(H')$，它是 H 吗？

不一定，应是 $\sigma^{-1}(H')=HN$。

证明：因 $\sigma(HN)=\sigma(H)\sigma(N)=\sigma(H)$，所以 $HN\subseteq\sigma^{-1}(\sigma(H))$。

任取 $a\in\sigma^{-1}(\sigma(H))$，必有 $\sigma(a)=h'\in\sigma(H)$，因为 $\sigma(H)$ 是 H 的象集，必有 $h\in H$，使 $\sigma(h)=h'=\sigma(a)$，即 $\sigma(h^{-1}a)=\sigma(h)^{-1}\sigma(a)=1'$，所以 $h^{-1}a\in N$，即 $a\in hN$，有 $a\in HN$，故 $\sigma^{-1}(\sigma(H))\subseteq HN$，所以原式成立。

(4) 若 $N\subseteq H$，则 $\sigma^{-1}(\sigma(H))=H$。

证：因 N 中有 1，故 $H=H\{1\}\subseteq HN\subseteq HH=H$

所以，$HN=H$，由(3)，结论成立。

(5) 先给 G' 子群 H'，$\sigma^{-1}(H')=H$ 再看 H 的象集 $\sigma(H)=\sigma(\sigma^{-1}(H'))$ 它是 H' 吗？答：是的。

证：因 $\sigma^{-1}(H')$ 表示 H' 在 G 中全体原象集，故在 σ 下再看象集必是 H'。

(6) 若 H 是 G 正规子群，则 $H'=\sigma(H)$ 是 G' 正规子群。

证：对任 $g'\in G'$ 往证 $g'H'g'^{-1}\subseteq H'$

因为必有 $g\in G$ 使 $\sigma(g)=g'$

而 $g'H'g'^{-1}=\sigma(g)\sigma(H)\sigma(g)^{-1}=\sigma(gHg^{-1})=\sigma(H)=H'$

所以，H' 正规子群。

(7) 若 H' 是 G' 的正规子群，则 $H=\sigma^{-1}(H')$ 是 G 的正规子群。

证：对任 $g\in G$ 要证 $gHg^{-1}\subseteq H$

因 $\sigma(gHg^{-1})=\sigma(g)\sigma(H)\sigma(g)^{-1}=g'H'g'^{-1}=H'$

所以，$gHg^{-1}\subseteq\sigma^{-1}(H')=H$

由(1)～(7)，可得如下定理：

定理5　若$G\sim G'$核N，则G与N之间的子群和G'（与(1)间）的子群一一对应，大群对应大群，小群对应小群，正规子群对应正规子群。

习　　题

1. 设σ是G到G'的同态映射，其核为N。若H是G的子群，求证$\sigma(H)$是G'的子群。若H'是G'的子群，求证$\sigma^{-1}(H')$是G的子群，求证$\sigma^{-1}(\sigma(H))=HN$，$\sigma(\sigma^{-1}(H'))=H'$。因此，若$N\subseteq H$，则$\sigma^{-1}(\sigma(H))=H$。由此说明$G'$的子群和包含$N$的$G$的子群一一对应。

2. 设σ是G到G'上的同态映射，τ是G'到G''上的同态映射。说明$\tau\sigma$是G到G''上的同态映射，并说明$\tau\sigma$的核为$\sigma^{-1}\tau^{-1}(=1'')$，其中$1''$是$G''$的壹。

3. 设σ是G到G'上的同态映射，H是包含σ的核N的G的正规子群，$H'=\sigma(H)$。求证H'是G'的正规子群并证明"第一同构定理"：$G/H\cong G'/H'$。

4. 设H和N都是G的正规子群，$N\subseteq H$，由第一同构定理推出

$$\frac{G}{H}\cong\frac{G/N}{H/N}$$

5. 设N是G的正规子群，H是G的任意子群，求证"第二同构定理"

$$\frac{HN}{N}\cong\frac{H}{H\cap N}$$

提示：用σ代表G到G/N的同态映射，σ引起H到HN/N的一个同态映射，求其核。

6. 用习题5证明四次对称群对*Klein*四元群的商群和三次对称群同构。

§5　环

定义　设R是一个非空集合，其上有两种代数运算(不妨叫加、乘，其中加用"+"，乘省略)。R叫做一个环，如果

(1) $a+b=b+a$，

(2) $a+(b+c)=(a+b)+c$，

(3) R中有一个元素0，适合$a+0=a$，

(4) 对于R中任意a，有$-a$，适合$a+(-a)=0$，

(5) $a(bc)=(ab)c$，

(6) $a(b+c)=ab+ac$，$(a+b)c=ac+bc$。

(1)到(4)说明R对于加法构成一个Abel群，(5)表示乘法适合结合律，(6)表示乘法对于加法有分配律；由于乘法不见得适合交换律，所以分配律有两个。

例如，全体整数普通加、乘；

实数域上n阶方阵，按矩阵加、乘，乘法无交换性；

$\{\bar{0},\bar{1},\bar{2},\bar{3}\}$按模4加、模4乘，成为4元有限环；

只取一元素0组成的集合，按普通加乘成为一个平凡环。

关于环的简单性质：

1. $a(b_1 + \cdots + b_n) = ab_1 + \cdots + ab_n$

$(a_1 + \cdots + a_m)b = a_1b + \cdots + a_mb$

$$\sum_{i=1}^{m}a_i\sum_{j=1}^{n}b_j = \sum_{i,j}a_ib_j$$

所以，当 m 为正整数时，$a,b\in$ 环 R，

$a(mb)=(ma)b=m(ab)$，并且规定 $0a=0$，其中第一个 0 是整数，第二个 0 是环中单位元。

因为乘法有结合律，所以 $a_1\cdots a_n$ 有意义，则 a^n 有意义，容易说明 $a^{m+n}=a^m\cdot a^n$，$(a^m)^n=a^{mn}$。

2. $a0=0$　说明环中任一元素与环中加单位元做乘法，结果是加单位元。

证：今后按习惯 $a+(-b)$ 记为 $a-b$

现在 $ac=a(c+0)=a(c+b-b)$

$=a[(c-b)+b]=a(c-b)-ab$

两边加 $(-ab)$ 得，$ac-ab=a(c-b)$

令 $b=c=0$ 得 $a(0-0)=a0-a0=0$

同理可证 $0a=0$

3. $(-a)b=a(-b)=-ab$，$(-a)(-b)=ab$

证：$(-a)b+ab=(-a+a)b=0b=0$

这说明 ab 与 $(-a)b$ 互为负元，即 $(-a)b=-ab$

同理知 $a(-b)=-ab$

而 $(-a)(-b)=-[a(-b)]=-[-ab]=ab$

所以对任意整数 m 有

$a(mb)=(ma)b=m(ab)$

按照 R 的乘法性质，我们区分下列各种环：

(一) 交换环

如果乘法适合交换律：

$$ab = ba$$

则 R 说是一个交换环。在交换环中，有第三指数律：

$$(ab)^n = a^nb^n$$

而且用数学归纳法可证二项式定理

$$(a + b)^n = a^n + na^{n-1}b + \cdots + b^n$$

(二) 有 1 环

如果 R 不只有一个元素而且乘法有单位元(记为 1)适合

$$a1 = 1a = a$$

则我们说 R 是有 1 环。

例如，偶数环是无 1 环，整数环是有 1 环。

有 1 环中 1 是唯一确定的。因若又有 $1'$，则 $1=11'=1'$；设 R 有 1，则 $1\neq 0$，即乘法单位 1 与加法单位 0 不同，因至少有二元，可取不为 0 的 a，$a\neq 0$，若 $1=0$ 则 $a=a1=a0=0$ 矛盾。

又如，任意无壹环可嵌入有壹环中，即无壹环 R 可扩充为有壹环 R^+(嵌入、扩充意为使 R 成为 R^+ 的子环，子环即对环中加乘仍为环的一个子集)。

证明：现设环 R 是无壹环，I 为整数环。

做如下形式元素 $a+m$，其中 $a\in R, m\in I$

（这里＋应理解为连系 R 中 a 与 I 中 m 的形式记号，也可记为 (a,m) 不用"＋"号）

规定加法、乘法为 $(a+m)+(b+n)=(a+b)+(m+n)$，$(a+m)(b+n)=(ab+na+nb)+mn$。

可以验证所有这些元素做成环 R^+。

因为 $(s+m)(0+1)=(a0+1a+m0)+m=a+m$

$(0+1)(a+m)=a+m$

所以其壹是 $0+1$。而且 $R^+\supseteq\{a+0|a\in R\}=R+0$

显然 $a+0\leftrightarrow a$，是 $R+0$ 与 R 的同构映射，可说 $R+0$ 就是 R，即 R^+ 包含 R。

注意，对于乘法群，其壹恒与子群的壹一致；但对于环，其壹却未必与子环的壹一致。

例如，任意域 F 上的所有 $n(>1)$ 阶方阵作成的环，有壹

$$I_n=\begin{pmatrix}1&0&\cdots&0\\0&1&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&\cdots&0&1\end{pmatrix}$$

所有如下形状的 n 阶矩阵

$$\begin{pmatrix}a&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&\cdots&0&0\end{pmatrix}\qquad a\in F$$

作成一个子环，有壹

$$\begin{pmatrix}1&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&\cdots&0&0\end{pmatrix}\neq I_n=\begin{pmatrix}1&0&\cdots&0\\0&1&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&\cdots&0&1\end{pmatrix}$$

又如，整数模 6 环，$R_6=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$ 有壹，子环 $\{\bar{0},\bar{2},\bar{4}\}$ 有壹 $\bar{4}$。

（三）无零因子环（消去环）

零因子：环 R 中若 $a\neq0, b\neq0$，但 $ab=0$，则说 a 是左零因子，b 是右零因子，R 说是有零因子环，若无上述性质元素，则 R 说是无零因子环。

例如：设 $R=\{\begin{pmatrix}a&0\\b&0\end{pmatrix}|a, b$ 是实数$\}$，易证对矩阵加乘 R 为环。

因 $\begin{pmatrix}1&0\\f&0\end{pmatrix}\begin{pmatrix}0&0\\c&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}\quad(c\neq0)$

所以 $\begin{pmatrix}1&0\\f&0\end{pmatrix}$ 是左零因子，$\begin{pmatrix}0&0\\c&0\end{pmatrix}$ 是右零因子。

但 $\begin{pmatrix}1&0\\f&0\end{pmatrix}$ 不一定是右零因子，因为，如果 $a\neq0$

$$\begin{pmatrix}a&0\\b&0\end{pmatrix}\begin{pmatrix}1&0\\f&0\end{pmatrix}=\begin{pmatrix}a&0\\b&0\end{pmatrix}\neq0$$

故存在环 R，其中某元素为左零因子，但不为右零因子。

又如：2×2 方阵为零因子⇔奇异

证：(⇒)设 A 为左零因子，要证 $|A|=0$

若不然 $|A|\neq 0$　A 为左零因子，必有 $B\neq 0$ 使 $AB=0$

因 $|A|\neq 0$ 则存在 A^{-1} 用 A^{-1} 左乘 $B=0$，矛盾。

A 为右零因子同理可证。

(⇐)如果 $|A|=0$，$A\neq 0$，则 A 可做左零因子如下：

看方阵 $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

有非零解的充分必要条件为 $\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}=0$

所以 A 可做左零因子，同理可证 A 可做右零因子。这表明，奇异矩阵即可是左因子，又可是右零因子。

(四) 整区

有壹无零因子的交换环叫做整区。

例如：所有整数、所有有理数、所有实数、所有复数作成的环是整区。

(五) 体

如果去掉 0，R 的其余元素作成一个乘法群，则称 R 为体。体有壹而且无零因子，其中任意非零元素有逆。域就是交换体，在域中，ab^{-1} 可以写成 a/b。

例如，取三个符号 $\boldsymbol{i}$、$\boldsymbol{j}$、$\boldsymbol{k}$，以实数 a、b、c、d 为系数而作如下形式的线性组合：

$$a+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k}$$

这种形式的线性组合叫做一个四元数，看所有四元数的集合。

规定两个四元数相加只要把它们相应的系数相加；i、j、k 之间的乘法如下：

×	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

两个四元数相乘只要按组合律展开再用上列乘法表化去 $\boldsymbol{i}$、$\boldsymbol{j}$、$\boldsymbol{k}$ 的乘积而且并项，可证所有四元数作成一个环，此环是一个体，但却不满足交换律，所以不是域。

定义　环 R 的子集 S，如果按 R 中的加、乘做成一个环，则称 S 为 R 的子环。体 K 的一个子环，若仍为体，则叫子体；若又为域，则叫子域。同样，对于域 F，也可以有 F 的子环、子域等。

定理 2′　环 R 的子集 S 作成子环，必要而且只要：

(1) S 非空；

(2) 若 $a\in S$，$b\in S$，则 $a-b\in S$；

(3) 若 $a\in S$，$b\in S$，则 $ab\in S$。

习　题

1. 若对所有 $a\in R$，$ea=a$，则 e 叫做 R 的一个左壹；若对所有 $a\in R$，$ae'=a$，则 e' 叫 R 的一

个右壹。求证若 R 有左壹也有右壹，则所有左壹右壹都相等，因而 R 中有一个唯一确定的壹。

2. 设 R 有壹。若 $ab=1$，则 a 叫 b 的左逆，b 叫 a 的右逆。求证若 a 有左逆又有右逆，则所有左逆右逆都相等，因而 a 有一个唯一确定的逆。

3. 求证任意无零因子的有限环必是一个体，假定环中不只有一个元素。

4. 在域中，证明若 $b\neq 0$，$d\neq 0$，则 $a/b=c/d$ 必要而且只要 $ad=bc$，而且

$$(a/b)\pm(c/d)=(ad\pm bc)/bd,\ (a/b)(c/d)=(ac)/(bd),\ (a/b)^{-1}=b/a$$

对于最后一式自然假定 $a\neq 0$。

5. 设 R 是一个环，P 是 R 的子集。说明 P 是 R 的子环必要而且只要

(1) $a\in p,b\in p$，则 $a-b\in p$

(2) $a\in p,b\in p$，则 $ab\in P$

(3) P 非空。

§6 环 同 态

定义 设 R 是一个环，R 的一个子集 N 说是 R 的一个理想子环，简称理想，如果：

(1) N 非空；

(2) 若 $a\in N,b\in N$，则 $a-b\in N$；

(3) 若 $a\in N,x\in R$，则 $ax\in N,xa\in N$。

易见，理想为子环，子环未必是理想。

例如，$I[x]$ 表示所有整系数多项式环，I 是整数环，所有整数可看作一次项以上系数全 0 的多项式，可见 I 是 $I[x]$ 子环，但不是理想，因若取 $2\in I$，$x\in I[x]$，$2x\notin I$，若取 N 为常数项为零的所有多项式，则任取 $f,g\in N$，$f-g\in N$，$fg\in N$，任取 $\varphi\in I[x]$，$f\varphi\in N$，所以，N 为理想。

又如，令 R 为偶数环，$N=\{6K\ K$ 是整数$\}$

则对任 $a,b\in N$，$a=6K,b=6K$，$a-b=6(K_1-K_2)\in N$。

任取 $a\in N,x\in R$，则 $ax=6K_12K_2=6(2K_1+K_2)\in N$，所以，$N$ 是理想。

再如，$N=\{0\}$ 和 $N=R$ 是两个平凡理想。

命题 设是 R 有壹交换环，$a\in R$，则 aR 是 R 的理想（aR 代表 a 与 R 中的所有元素按环乘法相乘所得的集合）。

证：aR 非空显然，对 aR 中任意二元，设为 ar_1,ar_2，则

$$ar_1-ar_2=a(r_1-r_2)\in aR$$

又因对 aR 中任意一元素 ar 以及 R 中任意一元素 x，有 $(ar)x=a(rx)\in aR$，所以 aR 为理想。

定义 设 R 是环，S 为 R 子集，R 中含 S 的最小理想，称 R 中 S 生成的理想。由一个元素 a 生成的理想叫主理想，记为 (a)。

显然，在有壹交换环中，$aR=(a)$。

例如，整数 a 的所有倍数 na 作成 I 的一个理想，记为 aI 或 (a)，叫做由 a 生成的理想。

又如，在偶数环 R 中，偶数 a 的所有偶数倍 $2na$ 作成 R 的一个理想，记为 aR；而偶数 a 的所有整数倍 na 作成一个主理想，记为 (a)，它是由 a 生成的主理想。从而可以看出 aR 与 (a) 并不相同，一般地，$aR\subseteq(a)$。

命题 若 R 是有壹交换环，则 $aR=(a)$。

证明：aR 指 a 的所有"倍元素"，而 (a) 当然要有 a 的所有倍元素，所以，$aR\subseteq(a)$。

另一方面，R 中有壹，故 aR 中有 a，已经证明 aR 是理想，所以，aR 是含 a 的理想，而 (a) 是含 a 的最小理想，所以，$(a)\subseteq aR$。证毕。

定义　设 R 是一个环，N 是一个理想，对于 $a,b\in R$，如果 $a=b+n,n\in N$，则我们说 a 和 b 模 N 合同，记为 $a\equiv b(\mathrm{mod}\ N)$。

这不过是加法群 R 中模加法子群 N 的合同关系。所以可将 R 分为 N 的陪集，N 的一个陪集叫 N 的一个剩余类，若 a 是 R 的任意元素，则包含 a 的剩余类可以写成 $a+N$ 的形式。a 和 b 在同一剩余类，当且仅当 a 和 b 模 N 合同。

如果 R 是有壹的交换环，而 N 是主理想，$N=(c)$，则 a 和 b 模 N 合同也可以说是模 c 合同，记为

$$a\equiv b(\mathrm{mod}\ c)。$$

例如，设 R 为整数环 I，$N=(m)=mI$，则 $a\equiv b(\mathrm{mod}\ N)$，即 $a-b\in mI$ 或 $m|a-b$ 或 $a\equiv b\ (\mathrm{mod}\ m)$。

和在整数合同中讨论的一样，我们有：

定理 1　在环 R 中，对于模 N，有

(1) 反身性：$a\equiv a$；

(2) 对称性：若 $a\equiv b$ 则 $b\equiv a$；

(3) 传递性：若 $a\equiv b,b\equiv c$，则 $a\equiv c$；

(4) 加法同态性：若 $a\equiv b,c\equiv d$，则 $a\pm c\equiv b\pm d$；

(5) 乘法同态性：若 $a\equiv b,c\equiv d$，则 $ac\equiv bd$。

证明：(1)到(4)在群中已讨论过，现只证(5)

因为 $a=b+n_1,c=d+n_2,n_1\in N,n_2\in N$，于是，$ac=bd+bn_2+n_1d+n_1n_2$，

因为 N 是理想，所以 $bn_2,n_1d,n_1n_2\in N$，即 $bn_2+n_1d+n_1n_2\in N$，所以，$ac\equiv bd$。证毕。

从证明中可以看出若 N 只是一般子环，而不是理想则不行。

定义　设 R 是一个环，S 是有加法和乘法两种代数运算的系统。R 到 S 中的一个映射 σ 说是环 R 到 S 中的一个同态映射，如果 $\sigma(a+b)=\sigma(a)+\sigma(b)$，$\sigma(ab)=\sigma(a)\sigma(b)$。若 σ 是环 R 到系统 R' 上的一个一对一的同态映射，则称 σ 是 R 与 R' 上的一个同构映射或同构对应。若 R 到 R' 上有一个同构映射，则称 R 与 R' 同构，记为 $R\cong R'$；若 R 到 R' 上有一个同态映射，则称 R 与 R' 同态，记为 $R\sim R'$。

类似群中的证明，我们有以下定理：

定理 2　设 R 是一个环，S 是一个有加法和乘法的运算系统。若 σ 是 R 到 S 中的一个同态映射，则 R 的映象 $R'=\sigma(R)$ 也是一个环。$\sigma(0)$ 就是 R' 的零 $0'$，$\sigma(-a)=-\sigma(a)$。若 R 有壹而 R' 不只有一个元素，则 R' 有壹而且 $\sigma(1)$ 就是 R' 的壹 $1'$；若 $a\in R$ 有逆，则 $\sigma(a)$ 在 R' 中有逆而且 $\sigma(a^{-1})$ 就是 $\sigma(a)^{-1}$。

定义　设 σ 是 R 到 R' 上的同态映射，R' 的零 $0'$ 的逆映象 $\sigma^{-1}(0')$ 叫 σ 的核。

定理 3　同态映射 σ 的核 N 是 R 的一个理想，设 a' 是 R' 的任意元素，则 a' 的逆映象 $\sigma^{-1}(a')=\{a\in R|\sigma(a)=a'\}$ 是 N 的一个剩余类。

证明：因为 σ 是 R 的加法群到 R' 的加法群上面的一个同态映射，我们有核 $N=\sigma^{-1}(0')$ 是 R 的子群且任 a' 的原象集 $\sigma^{-1}(a')$ 是模 N 的一个剩余类。下面证 N 为理想，只需证若 $a\in N$，$x\in R$，则 $ax\in N$，$xa\in N$ 即可。事实上，$\sigma(ax)=\sigma(a)\sigma(x)=0'\sigma(x)=0'$。所以，$ax\in N$，同理 $xa\in N$。证毕。

同样，我们要问：对于 R 的任意理想 N，是否有一个环 R' 而且有 R 到 R' 的一个同态映射 σ 使 N 恰为 σ 的核呢？回答也是肯定。

由群中已证结果知，模 N 的所有剩余类按照剩余类的加法作成一个加法群，即商群 R/N，规定 $\sigma(a)=a+N$，即 $\sigma:a\to a+N$，这样规定的 σ 便是群 R 到群 R/N 上的一个同态映射，其核为 N。为了使 R/N 成环，需要在剩余类间合理定义乘法。(怎样定义呢？若沿用陪集乘法，规定两剩余类 A 与 B 之积 AB 就是 A 中元与 B 中元按环中乘法所得的所有积作成的集合不行，见习题 5)我们规定乘法如下：设 $A=a+N$，$B=b+N$ 是两个剩余类，则积 $C=AB$ 规定为 $ab+N$，即 $(a+N)(b+N)=ab+N$。下面说明规定的合理性：

因为若在 $a+N$ 中另取 a_1，$b+N$ 中另取 b_1，这时 $a\equiv a_1$，$b\equiv b_1$ 则 $ab\equiv a_1b_1$，这说明含 ab 与含 a_1b_1 的剩余类是相同的，可见乘积由 A,B 确定与所选代表元无关。现由 σ 的定义知：$\sigma(a)=a+N$，$\sigma(b)=b+N$，$\sigma(ab)=ab+N=(a+N)(b+N)=\sigma(a)\sigma(b)$，所以，$\sigma$ 是环 R 到 R/N 上的一个同态映射，即 R/N 是环。所以有如下定理：

定理 4 按照剩余类的加法和乘法，R 对于理想 N 的所有剩余类的集合 R/N 是一个环，规定 $\sigma(a)=a+N$，则 σ 是 R 到 R/N 上的一个同态映射，其核为 N。R/N 叫做 R 对于 N 的剩余环。

定理 5 若 σ 是环 R 到 R' 上的一个同态映射，其核为 N，则 R' 与 R/N 同构：$R'\cong R/N$。

证明：设 a' 是 R' 的任意元素，则 $\sigma^{-1}(a')$ 是 N 的一个剩余类 A。规定 $\sigma:a'\leftrightarrow A$ 是 R' 到 R/N 的一一对应。设

$$\tau(a')=\sigma^{-1}(a')=a+N=A,\tau(b')=\sigma^{-1}(b')=b+N=B$$

因 $\sigma(a+b)=a'+b'$，$\sigma(ab)=a'b'$，故

$$\sigma^{-1}(a'+b')=a+b+N=A+B$$

$$\sigma^{-1}(a'b')=ab+N=AB$$

于是 $\tau(a'+b')=\sigma^{-1}(a'+b')=A+B=\tau(a')+\tau(b')$

$\tau(a'b')=\sigma^{-1}(a'b')=AB=\tau(a')\tau(b')$

故 τ 是 R' 到 R/N 上的一个同构映射。证毕。

例如，整数环 I，$m\in I$，$mI=(m)$ 是主理想，剩余环 $I/m\ I$ 是模 m 所有剩余类，每个剩余类也可等置为一代表元。若 $m=4$，剩余类是

$\{\cdots\cdots,-4,0,4,\cdots\cdots\}$

$\{\cdots\cdots,-3,1,5,\cdots\cdots\}$

$\{\cdots\cdots,-2,2,6,\cdots\cdots\}$

$\{\cdots\cdots,-1,3,7,\cdots\cdots\}$

$I/4I$ 由上面四个剩余类组成。现在等置为 $\bar{0},\bar{1},\bar{2},\bar{3}$，，剩余环是 $\{\bar{0},\bar{1},\bar{2},\bar{3}\}$，其中加乘运算模 4 进行。

至此，我们把数论中的合同概念推广到任意环上。而且还引进了剩余环的概念。完全和群论中的事实相对应，现在我们有：

定理 6 设环 R 同态于 R'：

$$R\sim R'$$

于是 R 与 N 之间的子环与 R' 的子环一一对应，大环对应大环，小环对应小环，理想对应理想。

特别，若 R' 与 $\{0\}$ 间无理想，则 R 与 N 间也无理想。

定义 一个环 R 叫单纯环，如果 R 除自己和 $\{0\}$ 外没有别的理想。例如 $\{\bar{0},\bar{1},\bar{2}\}$；环 R 的一

个理想 N 说是一个极大理想，如果 $N\subset R$，而 R 与 N 之间没有别的理想。

例如，整数环中 $5I=\{\cdots\cdots-6,-3,0,3,6,\cdots\cdots\}$是极大理想。

整数环中 $6I=\{\cdots\cdots-6,0,6,\cdots\cdots\}$不是极大理想。

设 I 整数环，$m\in I$，$mI=(m)$，则 mI 是极大理想$\Leftrightarrow m$ 是质数。

证明：($\Rightarrow$)若不然 $m=m_1m_2$ 且 $1<m_1,m_2<m$。看 m_1 生成的主理想$(m_1)=m_1I$，mI 中任一元可记为 ma，$a\in I$，$ma=m_1m_2a=m_1(m_2a)\in m_1I$，所以 $mI\subseteq m_1I$，又因 $m_1\notin mI$，所以 $mI\subset m_1I$，矛盾于 mI 是极大理想。

($\Leftarrow$)若 m 是质数，$I/mI=\{\bar{0},\bar{1},\cdots,\overline{m-1}\}$其加群元数是质数，所以除$\{\bar{0}\}$和 I/mI 外无真子群，故无真子环。当然无理想，又因 $I\sim I/mI$，而 I/mI 与$\{0\}$间无理想，所以 I 与 mI 间无理想，即 mI 为极大理想。

定理 7 若 $N\subset R$，则 N 是 R 的极大理想必要而且只要 R/N 是单纯环。

证明：因为 $R\sim R/N$，

所以 N 是极大理想$\Leftrightarrow R$ 与 N 间无理想

$\Leftrightarrow R/N$ 无真理想

$\Leftrightarrow R/N$ 是单纯环

定理 8 任意有壹的交换的单纯环 R 是一个域。

证明：只需证 R 中任意非零元有逆。

设 $a\neq0$，$a\in R$，看 $aR=(a)$，因为 $a\neq0$，又 $a\in aR$，故 $aR\neq\{0\}$。但 R 为单纯环，故 $aR=R$。又因 R 有壹，故必有 R 中之元素 b 适合 $ab=1$，即 a 在 R 中有逆 b。证毕。

定理 9 任意域 F 是有壹的交换的单纯环。

证明：只需证 F 是单纯环即可。

设 N 是 F 的任意理想，且 $N\neq\{0\}$，则任取 $a\in N$，$a\neq0$，因 F 中有 a^{-1}，所以 $aa^{-1}=1\in N$，任取 $x\in F$，因 N 为理想，所以 $x=1x\in N$，所以 $F\subseteq N$，但因 $N\subseteq F$ 故 $N=F$，所以 F 为单纯环。

定理 10 设 R 是有壹的交换环，N 是 R 的理想，于是 R/N 是一个域，必要而且只要 N 是一个极大理想。

证明：R/N 是一个域$\Leftrightarrow R/N$ 是一个有壹的交换的单纯环

$\Leftrightarrow N$ 是 R 的极大理想。

习 题

1. 设 K 是一个体而 K 同态于 R，求证 R 或只有一个元素 0 或和 K 同构。

2. 列举 $I/12I$ 的所有理想。

3. 设 F 是一个域，求证多项式环 $R[x,y]$中所有常数项为 0 的多项式作成一个理想，但不是主理想。

4. 说明在剩余环 I/mI 中，和 m 互质的所有剩余类作成一个乘法群，这样看来，群论中什么定理是 Fermat－Euler 定理的推广？

5. 设 A，B 是理想 N 在环 R 中的两个剩余类，命 P 为所有 ab 的集合，$a\in A$，$b\in B$，则自然 $P\subseteq AB$。举例说明 P 不见得等于 AB。

6. 设 α 是 R 到 R'上面的同态映射，N 是 R'的理想，求证 $\alpha^{-1}(N)$是 R 的理想。

第七章 多项式 有限域

§1 域的特征 素域

定义 若有壹交换无零因子环 R 的任意理想都是主理想，则称 R 为主理想环。

例如，整数环 I 是主理想环。

（主理想是理想，但理想未必是主理想。如，所有两个文字的多项式，按多项式加乘是环，所有常数项为 0 的多项式组成的集合是理想，但不是主理想，所有各项中均有文字 x 的多项式组成的集合是主理想 $xf[x,y]$）。

证明：须证 I 的任意理想 N 是主理想，若 $N=\{0\}$ 显然成立。

现设 N 中不只有一个元素，则在 N 中必有一个绝对值最小的非零元素，设为 a，显然 a 生成的理想 $(a)=aI\subseteq N$。

另一方面，任取 $b\in N$，若 $b=aq+r,0\leqslant r<|a|$，因为 $b,aq\in N$，所以 $r=b-aq\in N$，但 a 绝对值最小，只能 $r=0$，这样 $b=aq\in aI$，所以 $N\subseteq aI$，于是 $N=aI$ 是主理想，证毕。

设有整数环 I，任意域 F，用 e 代表 F 的壹。对于任意整数 m,n 我们有

$$(m+n)e=me+ne,$$
$$(mn)e=(me)(ne)。$$

因此，若规定 $\sigma(n)=ne$，则 σ 是 I 到 F 内同态映射。考查 $\sigma:I\sim F$，设 N 是其核，因为 N 是 I 的一个理想，又已知整数环 I 是主理想环，所以核 N 是主理想，设这理想由整数 p 生成，于是 $N=(p)=pI$，数 p 只与域 F 有关，称为域 F 的特征。

若 $p=0$，则 $ne=0\Leftrightarrow n=0$。

证：$(\Rightarrow)$ 若 $p=0$，则核 $N=\{0\}$，

若 $ne=0$，则 $\sigma(n)=0$，

所以 $n\in N$，即 $n=0$。

$(\Leftarrow)$ 显然。

这表明此时 e 在加法群中的周期是 0（或∞）。

若 $p>0$，则 $ne=0\Leftrightarrow p|n$。

证：$(\Rightarrow)$ 若 $ne=0$，即 $\sigma(n)=0$，于是 $n\in N=pI$，因为 pI 中任意元是 p 的倍数，故 $p|n$。

$(\Leftarrow)$ 若 $p|n$，则 $n\in N$，所以 $\sigma(n)=ne=0$。

这表明此时 e 在加法群中的周期是 p。

例如，域 F 中任意非零元在加群中周期也是 p。

证明：设 $a\in F,a\neq0$，则 $(na)e=a(ne)$，

因 a,e 都不是 0，而域中无零因子，所以 $ne=0\Leftrightarrow na=0$，而 e 的周期为 p，所以 a 的周期也为 p。

此例说明任意域中非零元在加群中周期相同，这样域 F 的特征也可定义为其中非零元在加群中的共同周期。

又如，$\{0,1,2,3,4\}$ 之特征为 5。

定理 1 任意域 F 的特征 p 是零或一个质数。

证明：若 $p\neq 0$，往证 p 是质数。

若不然，$p=hk$，$1<h<p$，$1<k<p$，

则 $(he)(ke)=(hk)e=pe=0$，

又因域中无零因子，则 (he)，(ke) 必有一为零，但 p 为 e 的周期，而 $k<p$，$h<p$，矛盾。证毕。

以上研究的是域的特征，但显然上述结果对无零因子环即可成立，一般来讲对无零因子环也可定义特征的概念。

定义 域 F 的子集按 F 加乘也为域，称 F 的子域。

当域 F 特征为质数 p 时，域 F 中含最小子域同构于 I/pI。

证明：看 $I\sim F$ 内的同态映射 σ，核为 pI，记同态象为 I'，

则 $I'=\sigma(I)=\{ne\mid n\in I, e$ 是 F 的乘法单位元$\}$，根据环同态基本定理（第六章 §6 定理 5）。

因 $I\sim I'$，得 $I'\cong I/pI$，容易证明 I/pI 是域，所以 I' 也为域，所以 I' 是 F 的子域。

又因 F 的任意子域要含 e，因此必含有 e 的所有倍数，即含有 I'，所以 I' 是域 F 的最小子域。

域上同态，或为同构，或所有元素对应 0。事实上体即有此结论（见第六章 §6 习题 1）。

当域 F 特征为 0 时，域 F 中含有的最小子域同构于有理数域 R_0。

证：现在要把已定义的同态扩大到 R_0 到 F 内。办法是规定 $\sigma(m/n)=(me)/(ne)$

(1)先说明规定的合理性

设 $h/k=m/n$，则 $hn=km$，

所以 $(he)(ne)=(ke)(me)$，

故 $(he)/(ke)=(me)/(ne)$，

可见规定与有理数表示无关，即规定合理。

(2)证同态性

$$\begin{aligned}\sigma(m/n+h/k)&=\sigma((km+hn)/nk)\\&=((km+hn)e)/((nk)e)\\&=((km)e+(hn)e)/((nk)e)\\&=((me)(ke)+(he)(ne))/((ne)(ke))\\&=(me)/(ne)+(he)/(ke)\\&=\sigma(m/n)+\sigma(h/k)\end{aligned}$$

$$\begin{aligned}\sigma((m/n)(h/k))&=\sigma((mh)/(nk))\\&=((mh)e)/((nk)e)\\&=((me)(he))/((ne)(ke))\\&=((me)/(ne))((he)/(ke))\\&=\sigma(m/n)\sigma(h/k)\end{aligned}$$

因为 $\sigma(n)=\sigma(n/1)=ne/e=(ne)e^{-1}=ne$，所以 R_0 到 F 内的映射是 I 到 F 内的映射的扩大，但 R_0 是一个域而 σ 不是把它的所有元素映成 0，如 $\sigma(1)=e\neq 0$，所以 σ 是同构映射。记 σ 下 R_0 的象为 R_0'，则 $R_0\cong R_0'$，因 F 的任意子域要包含 e，e 的整数倍及其商，即包含 R_0'，所以 F 包含和 R_0 同构的 R_0' 为其最小子域。

定义　最小域或素域指没有真子域的域，特征 p 的最小域为 R_p(p 为 0 或一质数)。

设 F 是最小域，当 F 特征为 0 时，它与有理数域同构，当 F 的特征为 p 时，它与模 p 剩余类域 I/pI 同构。也可以说，最小域就是有理数域或模 P 剩余类域。

例如，$p=5$，$I/5I=\{0,1,2,3,4\}$，其中加乘对 5 取模，-1 表示 1 的负元素，因 $1+4=0$，所以 $4=-1$。若引入记号 $\sqrt{-1}$，指自乘得 -1 的元素。因为 $-1=4$，$2^2=3^2=4$，所以 $\sqrt{-1}=2$ 或 3，而没有 $\sqrt{-2}$。

根据以上的讨论可得：

定理 2　设 p 为质数或等于 0，特征为 p 的任意域 F 包含 R_p 为其最小子域。

本定理是在同构观点下叙述的，任意域特征为 0 就可以认为是有理数域的扩域，特征 p 就认为是模 p 剩余类域的扩域。

设 n 是整数，F 是域，任取 $a\in F$，na 怎样理解呢？

(1) $n>0$，$na=a+\cdots+a$，$0a=0$，$(-n)a=-na$。

(2) 现在认为 R_p 是 F 子域，$p=0$ 时，n 可认为是有理数。于是可认为是 F 的元素，p 是质数时，n 可模 p 看，也是 F 中的元素，于是 na 可解释为 F 中两元素相乘，两种解释结果相同。但在无壹环中只能用第一种解释。

特征为 0 的域必为无限域；特征为 p 的域可有限，也可无限。

特征为质数 p 的域 F 的简单性质：

(1) 若 $a,b\in F$，则 $(a+b)^p=a^p+b^p$；

例如，在 R_2 上，$a^2+b^2=(a+b)^2$。

(2) $(a-b)^p=a^p-b^p$；

(3) $(a\pm b)^{p^n}=a^{p^n}\pm b^{p^n}$

(4) $(a_1+a_2+\cdots+a_n)^p=a_1^p+\cdots+a_n^p$

(5) 在(4)中令 $a_1=a_2=\cdots=a_n=1$。

则 $n^p=n$，n 非 0 时 $n^{p-1}=1$，此即 Fermat 定理。

习　　题

1. 在 R_{17} 中 $2/3$ 等于什么？

2. 在 R_5 中 $\sqrt{-1}$ 等于什么？R_{23} 中有没有 $\sqrt{-1}$？

3. 在 R_7 中利用公式

$$\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

解二次方程 $x^2-x+5=0$

4. 在 R_7 上求下列矩阵之逆：

$$\begin{pmatrix}2 & 3\\ 1 & 4\end{pmatrix}$$

5. 证明 R_2 上的四个矩阵

$$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix},\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix},\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$$

在矩阵的加法乘法下作成一个域。

6. 试看 R_7 上的所有“复数”：

$$a+b\sqrt{-1}$$

其中 a、b 在 R_7 中任意取值。这里共有 49 个数，象普通复数那样计算，求证这 49 个数作成一个域。

§2 多项式的整除性

定义 令 x 是一个抽象符号（或叫字母，文字，记号等），F 是一个域，$a_0,\cdots,a_n\in F$，*一元多项式*是如下形式的式子：

$$a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n \tag{1}$$

其中 n、$n-1$，…为非负整数，今后记为 $f(x)$、$g(x)$ 等。

其中文字在没有用域中元代入时是形式的式子，用域中元代入后，按域中加法乘法运算得域中一元。多项式中没有文字的项称为常数项。多项式中，系数是 0 的项可以删去，另一方面，也可以添上一些系数是 0 的项。例如：$2x^2-0x-1$ 可以写成 $2x^2-1$，$0x^3+2x^2-1$ 等。

定义 两个多项式 $f(x)$ 和 $g(x)$ 说是*相等的*，即

$$f(x)=g(x),$$

如果可以添上一些系数是 0 的项使两个多项式完全一样。

易见，1）多项式(1)等于 0 当且仅当所有系数 $a_0,\cdots,a_n$ 都是 0；

2）一个多项式 $f(x)\neq 0$ 总可化为(1)的形式且 $a_0\neq 0$。这时，a_0 和 n 是唯一确定的。

定义 若 $f(x)\neq 0$ 且已化为(1)的形式，其中 $a_0\neq 0$，那么，a_0 称为 $f(x)$ 的*首系数*，n 称为 $f(x)$ 的*次数*，常数多项式 0 的次数可以说是 $-\infty$。

例如，$0x^3+2x^2-1$ 的次数为 2；

4 的次数为 0。

$f(x)$ 的次数记为次 $f(x)$。

下面定义两个一元多项式 $f(x)$ 与 $g(x)$ 的加法及乘法：

$f(x)+g(x)$ 为把 $f(x)$ 与 $g(x)$ 的同次项的系数相加所得到的多项式；$f(x)g(x)$ 为以 $f(x)$ 的每一项乘 $g(x)$ 的每一项，然后合并同次项且以加号相连结所得到的多项式。可以验证，这样规定后，所有一元多项式作成一个有壹交换环。记为 $F[x]$。$F[x]$ 包含 F 为其子域。F 中的 0 就是 $F(x)$ 的零，F 中的 1 就是 $F[x]$ 的 1，$-f(x)$ 就是把 $f(x)$ 的所有系数取负所得到的多项式。

关于多项式的次数，我们有

$$次(f(x)+g(x))\leqslant \max(次 f(x)，次 g(x)) \tag{2}$$

$$次 f(x)g(x)=次 f(x)+次 g(x) \tag{3}$$

证：两个多项式相加不过是把对应的系数相加，不会得出比两个多项式中出现的项的次数还要高的项，所以(2)成立。若 $f(x)\neq 0$ 且 $g(x)\neq 0$，则可设

$$f(x)=a_0x^n+b_1x^{n-1}+\cdots+a_{n-1}x+a_n \qquad a_0\neq 0$$

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m \qquad b_0\neq 0$$

且次 $f(x)=n$，次 $g(x)=m$。今

$$f(x)g(x)=a_0b_0x^{n+m}+\cdots+a_nb_m$$

因 $a_0b_0\neq 0$，所以次 $f(x)g(x)=n+m=$ 次 $f(x)+$ 次 $g(x)$，故(3)成立。

若 $f(x)$，$g(x)$ 中至少有一个是多项式 0，则

$$f(x)g(x)=0, \text{即次} f(x)g(x)=-\infty,$$

但由于 $-\infty+m=-\infty$，

$n+(-\infty)=-\infty$，

$-\infty+(-\infty)=-\infty$，

所以，(3)仍成立。

定理 1　域 F 上 x 的多项式作成的环 $F[x]$ 是一个整区。

证明：只需证无零因子，即证当 $f(x)\neq 0$，$g(x)\neq 0$ 时，其积 $f(x)g(x)\neq 0$。

因为次 $f(x)\neq-\infty$，次 $g(x)\neq-\infty$，由(3)，

则 次 $f(x)g(x)=$ 次 $f(x)+$ 次 $g(x)\neq-\infty$，所以 $f(x)g(x)\neq 0$。

下面我们在域 F 上的多项式环 $F[x]$ 中讨论一些性质。

带余除法定理　对任意 $f(x)$，$g(x)$，存在 $q(x)$，$r(x)$ 使

$$f(x)=q(x)g(x)+r(x) \qquad \text{次} r(x)<\text{次} g(x) \tag{4}$$

且 $q(x)$，$r(x)$ 唯一。

证明：存在性，用长除法可求出 $q(x)$，$r(x)$。

唯一性，设存在另外的 $q_1(x)$，$r_1(x)$ 使

$$f(x)=q_1(x)g(x)+r_1(x) \qquad \text{次} r_1(x)<\text{次} g(x) \tag{5}$$

则由(4)，(5)有 $q(x)g(x)+r(x)=q_1(x)g(x)+r_1(x)$

从而 $(q_1(x)-q(x))g(x)=r(x)-r_1(x)$　(6)

若 $q_1(x)-q(x)\neq 0$，则次 $(q_1(x)-q(x))g(x)\geq$ 次 $g(x)$。

而次 $(r(x)-r_1(x))<$ 次 $g(x)$，与(6)矛盾。所以 $q_1(x)-q(x)=0$，即 $q_1(x)=q(x)$，故 $r(x)=r_1(x)$。

定义　若对 $f(x)$ 和 $g(x)$ 有 $h(x)$ 使

$$f(x)=h(x)g(x) \tag{7}$$

则我们说 $g(x)$ 整除 $f(x)$，记为 $g(x)|f(x)$，或说 $g(x)$ 是 $f(x)$ 的因式，$f(x)$ 是 $g(x)$ 的倍式。

定理 2　设 $g(x)\neq 0$，$g(x)|f(x)$ 当且仅当以 $g(x)$ 除 $f(x)$ 所得的余式为 0。

根据商和余式的唯一性很容易证明。

因一个文字的多项式的因式分解理论和整数的因数分解理论是平行的，所以整数中的一些事实在这里仍成立。我们这里略去证明部分。

1°　若 $f|g$，$g|h$，则 $f|h$。

2°　若 $f|g$ 则 $f|gh$。

3°　若 $f|g$，$f|h$，则 $f|g\pm h$。

4°　若 f 整除 $g_1,\cdots,g_n$，则 $f|h_1g_1+\cdots+h_ng_n$。

5°　若在一等式中，除某项外，其余各项都是 f 的倍式，则该项也是 f 的倍式。

6°　若 $f|g$，$g|f$，则 f 与 g 只差一个非 0 常数因子。

证明：仿照第五章§1 中有关性质的证明，只是在推出 $1=de$ 后推理如下：只有 d，e 都是非 0 常元素时此式才成立。

两个多项式，如果只差一个非 0 常数因子，则说它们是相通的。在因式分解问题中，相通的多项式可看作没有什么区别。

7° $a\in F, a\neq 0, a\mid f(x)$。

8° $f(x)\in F[x], f(x)\mid 0$。

定义 若 $d\mid f_1,\cdots,d\mid f_n$，则说 d 是 $f_1,\cdots,f_n$ 的公因式。d 称为 $f_1,\cdots,f_n$ 的最高公因，如果 d 是 $f_1,\cdots,f_n$ 的公因式，而且 $f_1,\cdots,f_n$ 的任意公因式整除 d。

9° 若 d 和 d' 都是 $f_1,\cdots,f_n$ 的最高公因，则 d' 和 d 相通。

定义 若 $f\mid g$，而 f 不是常数也不和 g 相通，则说 f 是 g 的一个*真因式*。

定义 设多项式 p 非常元素，p 说是一个*质式或不可约多项式*，如果 p 没有真因式。

定义 若 $f_1,\cdots,f_n$ 除了非 0 常元素外没有公因式，则说 $f_1,\cdots,f_n$ 是*互质的*。

换句话说，$f_1,\cdots,f_n$ 是互质的，当且仅当其最高公因为非 0 常元素，或说当且仅当其最高公因为 1。

用数论中的方法可类似地证明：

定理 3 任意多项式 f 和 g 必有最高公因。

定理 4 f,g 的最高公因 d 可以表为 f,g 的倍式和，即表为下面的形式：

$$d = \lambda f + \mu g$$

其中 λ,μ 都是多项式。

定理 5 若 p 是质式而 $p\mid f_1\cdots f_n$，则 p 整除 $f_1,\cdots,f_n$ 之一。

定理 6 任一非常数多项式恰有一法表为质式的乘积。

所谓“恰有一法”，当然是把相通的质式看作一样而且不考虑质因式的次序。

定理 7 任意非常数多项式 f 可以唯一地表为下面的形式：

$$f = c p_1^{r1} p_2^{r2} \cdots\cdots p_k^{rk}$$

其中 $p_1,p_2,\cdots\cdots,p_k$ 是互不相通的质式。$r1,r2,\cdots\cdots,rk$ 是正整数。

例如，域 F 上多项式 f,g 互质 $\Leftrightarrow$ 存在 λ,μ 使 $\lambda f+\mu g=1$。

证明：($\Rightarrow$)定理 4。

($\Leftarrow$)若不然，f,g 有公因式 d 且 d 不是非 0 常元素，由性质 4°有 $d\mid 1$，矛盾。

按照质式的定义易见，任意一次式必是质式，因而对 F 中任意元素 a，$x-a$ 是质式，而且 $a\neq b$ 时，$x-a$ 和 $x-b$ 不相通。可见，只要 F 中有无穷多个元素，$F[x]$ 中便有无穷多个不相通的质式，这也可以说是对应整数环中欧几里得关于质数无穷多的定理，但这是太简单了，我们应当进一步问：$F[x]$ 中有没有次数任意高的质式？以下几节内，将对一些特殊的域 F 回答这一问题。

另外，我们指出，定理 6 和定理 7 只说明多项式的质因式分解式在理论上是存在的，并没有给出“能行的”分解方法。在这一点上，多项式的因式分解和整数的因式分解是不同的，因为，任意正整数总可以通过以较小的数来试除的方法在有限步内分解为质因数的乘积。

习　　题

1. 在 R_5 上，试用综合除法求以 $x-2$ 除 $2x^5-x^4-2x^3+1$ 所得的商式和余式。

2. 若非常数多项式 $f(x),g(x)$ 互质，求证必有多项式 $\lambda(x),\mu(x)$ 使

$$\lambda(x)f(x) + \mu(x)g(x) = 1$$

且次 $\lambda(x)<$ 次 $g(x)$，次 $\mu(x)<$ 次 $f(x)$。进一步证明这样的 $\lambda(x),\mu(x)$ 是唯一的。

3. 用下列方法证明定理 3 和定理 4：试看所有形为 $\lambda f+\mu g$ 的非 0 多项式，命 d 为这些多

项式中次数最低的一个，证明 d 是 f,g 的最高公因。

4. 用类似上题的方法证明环 $F[x]$ 中任意理想必是主理想。

5. 求证：$\varphi(x)F[x]$ 是 $F[x]$ 的极大理想，当且仅当 $\varphi(x)$ 不可约。

6. 在 R_3 上，分解 x^4+x^3-x+1 为质因式的乘积。

§3　多项式的根

下面我们在任意域 F 上的多项式环 $F[x]$ 中讨论多项式的根。

定义　设 $f(x)\in F[x]$，$\alpha\in F$，以 α 代 $f(x)$ 中的 x，按 F 中加乘运算得值为 $f(\alpha)$。若 $f(\alpha)=0$，则我们说 α 是多项式 $f(x)$ 的一个根，或说 α 是方程 $f(x)=0$ 的一个根。

定理 1（**余式定理**）　以 $x-\alpha$ 除 $f(x)$ 所得的余式等于 $f(\alpha)$。

证明：设余式为 C，则根据带余除法定理有，

$$\text{次}\,C<\text{次}(x-\alpha),\text{但次}(x-\alpha)=1,$$

所以，次 $C<1$，即 C 是一个常元素，设商式为 $q(x)$，于是

$$f(x)=q(x)(x-\alpha)+C$$

以 α 代入，得 $f(\alpha)=q(\alpha)(\alpha-\alpha)+C$，所以 $C=f(\alpha)$。

推论　$x-\alpha\mid f(x)$，当且仅当 α 是 $f(x)$ 的根。

证明：$x-\alpha\mid f(x)\Leftrightarrow$ 余式为 0

$\Leftrightarrow f(\alpha)=0$

$\Leftrightarrow \alpha$ 是 $f(x)$ 的根。

定义　说 α 是非 0 多项式 $f(x)$ 的 k 重根，如果 $(x-\alpha)^k$ 整除 $f(x)$ 且 $(x-\alpha)^{k+1}$ 不整除 $f(x)$。若 $k>1$，则我们说 α 是 $f(x)$ 的重根。若 $f(x)$ 是多项式 0，则对任意正整数 k，$(x-\alpha)^k\mid f(x)$，所以我们说 α 是 $f(x)$ 的 ∞ 重根而且 α 也看作是 $f(x)$ 的重根。

定理 2　设非 0 多项式 $f(x)$ 的次数为 n，则 $f(x)$ 最多有 n 个根，此处 k 重根作为 k 个根计算。

证明：把 $f(x)$ 分为质因式的乘积形式：

$$f(x)=c(x-\alpha_1)^{k_1}\cdots(x-\alpha_r)^{k_r}p_1(x)\cdots p_s(x) \tag{1}$$

其中 $\alpha_1,\cdots,\alpha_r$ 都不同，而 $p_1(x),\cdots,p_s(x)$ 都是高于一次的质式。则

$$n=k_1+\cdots+k_r+\text{次}(p_1(x)\cdots p_s(x)) \tag{2}$$

显然，α_i 是 $f(x)$ 的 k_i 重根，$i=1,\cdots,r$。除了这些，$f(x)$ 没有另外的根 α，因否则 $x-\alpha$ 应是 $f(x)$ 的质因式，而分解式(1)中没有这个质因式。可见，当 k 重根算 k 个根时，$f(x)$ 共有 $k_1+\cdots+k_r$ 个根。由(2)$k_1+\cdots+k_r\leq n$，所以 $f(x)$ 最多有 n 个根。

这里的系数是在任意域中，可扩充到无零因子交换环中。但在有零因子环中不能成立，例如 x^2 在模 16 的环中有四个根 0，4，8，12，在非交换环中也不能成立，例如在四元数体中，对于多项式 $x^2+1=0$，$\pm i$，$\pm j$，$\pm k$ 等都是根。

定义　两个多项式 $f(x)$ 和 $g(x)$ 说是恒等，如果以 F 中任意元素 α 代 x，恒有：

$$f(\alpha)=g(\alpha)$$

比较一下这个定义和上节定义，我们看到，$f(x)$ 和 $g(x)$ 相等表示二者作为包含文字 x 的两个式子形式上完全相同，而 $f(x)$ 和 $g(x)$ 恒等表示二者作为变量 x 的两个函数恒取同样的值。两种观点是否一致呢？

定理3 设 F 中有无穷多个元素，$f(x)$ 和 $g(x)$ 恒等，当且仅当二者相等。

证明：($\Leftarrow$) 显然。

($\Rightarrow$) $f(x)$ 和 $g(x)$ 恒等。看 $f(x)-g(x)$，

因对任 $\alpha\in F$，$f(\alpha)=g(\alpha)$，即 $f(\alpha)-g(\alpha)=0$，

所以 $f(x)-g(x)$ 有无穷多根。由定理2知，只有0多项式有无穷多根，所以 $f(x)-g(x)=0$，即 $f(x)=g(x)$。

判定一个多项式有没有重根在一些问题中是很重要的。一般说来，具体求多项式的根没有能行的方法，我们看是否有简便的办法判定一个多项式有没有重根。

下面我们定义多项式 $f(x)$ 的微商 $f'(x)$ 如下：

$$\text{若 } f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$$

$$\text{则 } f'(x)=na_0x^{n-1}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$$

定理4 若 α 是非常数多项式 $f(x)$ 的 k 重根，则它至少是 $f'(x)$ 的 $k-1$ 重根。

证明：因为 α 是 k 重根，则 $f(x)=(x-\alpha)^kg(x)$，且 $x-\alpha$ 不整除 $g(x)$，所以

$$f'(x)=k(x-\alpha)^{k-1}g(x)+(x-\alpha)^kg'(x) \qquad (*)$$

当 k 是 F 的特征倍数时，($*$)式为 $f'(x)=(x-\alpha)^kg'(x)$。

所以，至少是 $f'(x)$ 的 $k-1$ 重根。

当 k 不是 F 的特征倍数时，($*$)式右边第一项非0，

所以 $f'(x)$ 只能被 $(x-\alpha)^{k-1}$ 整除，不能被 $(x-\alpha)^k$ 整除，

即恰是 $f'(x)$ 的 $k-1$ 重根。

所以 α 至少是 $f'(x)$ 的 $k-1$ 重根。

例如，在 $R_2[x]$ 中，$f(x)=x^3+x=x(x^2+1)=x(x+1)^2$

所以 $x=1$ 是二重根。

$$f'(x)=3x^2+1=x^2+1=(x+1)^2$$

所以 $x=1$ 仍是二重根。

$f''(x)=2x=0$，所以 $x=1$ 是 ∞ 重根。

定理5 α 是 $f(x)$ 的重根，当且仅当它是 $f(x)$ 和 $f'(x)$ 的公共根。

证明：($\Rightarrow$) 若 $f(x)$ 是0多项式，显然。

令 $f(x)\neq0$，因为 α 是 $f(x)$ 的重根，所以可说 α 是 $f(x)$ 的 k 重根，且 $k>1$，故 α 至少是 $f'(x)$ 的 $k-1$ 重根，且 $k-1\geq1$，所以 α 是 $f'(x)$ 的根，所以是 $f(x)$ 和 $f'(x)$ 的公共根。

($\Leftarrow$) 若不然，有二种情况，一种是 α 不是 $f(x)$ 的根，另一种是 α 是 $f(x)$ 的1重根。若 α 不是 $f(x)$ 的根，当然不会是公共根，矛盾，若 α 是 $f(x)$ 的1重根，而1不是 F 的特征的倍数，所以 α 是 $f'(x)$ 的 $k-1=0$ 重根，即 α 不是 $f'(x)$ 的根，当然不会是公共根，矛盾。

用辗转相除法求出 $f(x)$ 和 $f'(x)$ 的最高公因 $d(x)$，$d(x)$ 的根就是 $f(x)$ 的重根。只要看 $d(x)$ 在 F 中有没有根就知道 $f(x)$ 在 F 中有没有重根。

下面讨论复数域和实数域上的多项式。

定理6 复数域上，任意非常数多项式必有根。（代数学基本定理）

证明较长，略。

定理7 复数域上，只有一次式才是质式。因之，任意非常数多项式 $f(x)$ 可以唯一地分解成下面的形式：

$$f(x)=c(x-\alpha_1)^{k_1}\cdots(x-\alpha_r)^{k_r}$$

其中 $\alpha_1\cdots,\alpha_r$ 恰是 $f(x)$ 的所有不同的根，若重根按其重数计数，则 n 次多项式恰有 n 个根。

证明：(1)若不然，设 $g(x)$ 是质式，且次 $g(x)>1$，由定理 6，$g(x)$ 在复数域中有根，不妨设为 α，从而 $x-\alpha|g(x)$，故 $g(x)$ 不是质式，矛盾。

因复数域上，只有一次式才是质式，所以任意非常数多项式 $f(x)$ 可以唯一分解成下面的形式：

$$f(x)=c(x-\alpha_1)^{k1}\cdots\cdots(x-\alpha_r)^{kr}$$

且 α_i 是 $f(x)$ 的 ki 重根，$i=1,\cdots,r$，$f(x)$ 没有另外的根。若次 $f(x)=n$，则 $k1+\cdots+kr=n$，所以，重根按其重数计数时，$f(x)$ 恰有 n 个根。

定理 8　实数域上，质式只能是一次式或二次式。二次式 ax^2+bx+c 是质式，当且仅当判别式 $b^2-4ac<0$。

证明：设次 $g(x)>2$，若 $g(x)$ 有实根 α，则 $x-\alpha|g(x)$，故 $g(x)$ 非质式。

否则，把 $g(x)$ 看做复数域上的多项式，由定理 6，则 $g(x)$ 有虚根 $a+bi$，$b\neq0$，令

$$\begin{aligned}h(x)&=(x-(a+bi))(x-(a-bi))\\&=x^2-2ax+(a^2+b^2)\end{aligned}$$

则 $h(x)$ 是实系数多项式，且次 $h(x)=2$，

故可设 $g(x)=q(x)h(x)+cx+d$

以 $a+bi$ 代 x 得

$$0=0+c(a+bi)+d$$

即

$$c(a+bi)+d=0$$

从而 $cbi=0$，因为 $b\neq0$，所以 $c=0$。

所以 $d=0$，得 $g(x)=q(x)h(x)$，即 $h(x)|g(x)$，而 $h(x)$ 是实系数多项式，所以 $g(x)$ 非质式。

下面看二次式 ax^2+bx+c 是质式当且仅当此式无实根，由中学学过的知识知当且仅当 $b^2-4ac<0$。

§4　有理域上的多项式

上节中我们看到，复数域上只有一次式是质式，实数域上只有一次式和一部分二次式是质式，本节将说明，和上述两个数域不同，有理数域上有任意高次的质式。此外，我们附带讨论求有理根的问题。

设 $f(x)$ 为有理系数多项式，以适当的非 0 整数 c 来乘之。则可使 $cf(x)$ 是整系数多项式。因此，任意有理系数多项式和一个整系数多项式相通。

定义　设

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$$

是一个整系数多项式。若系数 $a_0,a_1,\cdots,a_n$ 互质(即除 ±1 外无公因数)，则称 $f(x)$ 是一个本原多项式。

设 $f(x)$ 是一有理系数多项式，用适当的 c 乘之，使得 $cf(x)$ 是一整系数多项式，然后，对 $cf(x)$ 的系数求出其最高公因 d，则 $(c/d)f(x)$ 是一本原多项式，由此可见，任意有理系数多项式与一本原多项式相通。

定理 1 设 p 是一个质数

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$
$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$$

是两整系数多项式，若 p 整除 $f(x)g(x)$ 的所有系数，则 p 或整除 $f(x)$ 的所有系数或整除 $g(x)$ 的所有系数。

证明：若不然，设 a_i 是 $f(x)$ 的系数中从后往前看第一个不为 p 整除者，于是，

$$p \text{ 不整除 } a_i, p\,|\,a_{i+1}, \cdots, p\,|\,a_n$$

类似地，设

$$p \text{ 不整除 } b_j, p\,|\,b_{j+1}, \cdots, p\,|\,b_m$$

现在看 $f(x)g(x)$ 中 $x^{n-i+m-j}$ 的系数，应为

$$a_ib_j + a_{i+1}b_{j-1} + a_{i+2}b_{j-2} + \cdots$$
$$+ a_{i-1}b_{j+1} + a_{i-2}b_{j+2} + \cdots$$

此式中，除 a_ib_j 外，其余各项都是 p 的倍数，而 p 不整除 a_i，p 不整除 b_j，得 p 不整除 a_ib_j（此处用到了 p 是质数）故 p 不整除 $x^{n-i+m-j}$ 的系数矛盾。证毕。

定理 2 设 $f(x)$ 是本原多项式，$g(x)$ 是整系数多项式，若 $f(x)\,|\,g(x)$（是在有理数域意义上）则以 $f(x)$ 除 $g(x)$ 所得之商式必是整系数多项式。

证明：因为 $f(x)\,|\,g(x)$，所以 $g(x)=f(x)h(x)$，需证 $h(x)$ 是整系数多项式，总可取常数 c 使 $ch(x)$ 是整系数多项式，记为 $k(x)=ch(x)$，所以 $cg(x)=f(x)k(x)$，又因 $f(x)$，$k(x)$，$g(x)$ 是整系数多项式，所以 c 整除 $f(x)k(x)$ 的所有系数。设 $c=p_1\cdots p_r$，p_i 为质数，所以 p_1 整除 $f(x)k(x)$ 的所有系数。由定理 1，p_1 或整除 $f(x)$ 的所有系数或整除 $k(x)$ 的所有系数。但 $f(x)$ 是本原多项式，所以 p_1 整除 $k(x)$ 的所有系数。即

$$k(x) = p_1k_1(x)$$

其中 $k_1(x)$ 是整系数多项式。故有

$$p_2\cdots p_r\,g(x) = f(x)k_1(x)$$

如此进行下去，得

$$g(x) = f(x)k_r(x)$$

其中 $k_r(x)$ 是整系数多项式，根据带余除法定理，$k_r(x)=h(x)$，所以 $h(x)$ 是整系数多项式。

定理 3 （Eisenstein 定则）设

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$

是整系数多项式，若对一个质数 p

$$p \text{ 不整除 } a_0, p\,|\,a_1, \cdots, p\,|\,a_n, p^2 \text{ 不整除 } a_n$$

则 $f(x)$ 在有理域上不可约（质式）。

证明：若不然，则 $f(x)$ 必有一真因式 $\varphi(x)$，因为 $\varphi(x)$ 和一个本原多项式相通，所以不妨假定 $\varphi(x)$ 是本原多项式，则 $f(x)=\varphi(x)\psi(x)$，由定理 2，$\psi(x)$ 是整系数多项式。令

$$\varphi(x) = b_0x^r + \cdots + b_r, \psi(x) = c_0x^s + \cdots + c_s$$

则

$$a_0x^n = b_0c_0x^{r+s} \quad a_n = b_rc_s$$

因为 p 不整除 a_0，所以 p 不整除 b_0，p 不整除 c_0，又因为 p^2 不整除 a_n，所以 p 至少不整除 b_r，c_s 中一个，不妨设 p 不整除 c_s，在 $b_0x^r+\cdots+b_r$ 中从后往前看，第一个不是 p 的倍数的系数为 b_i，

则看 $f(x)$ 中 x^{i+s} 的系数应为

$$b_ic_s + b_{i+1}c_{s-1} + b_{i+2}c_{s-2} + \cdots$$

由已知 p 应整除此系数，但 p 不整除 b_ic_s，而其余各项均为 p 的倍数。所以，p 不整除此系数，矛盾。

根据定理 3，我们可以写出许多有理域上不可约的多项式，例如 x^n-2，因为存在质数 2，2 不整除 1，$2|0,\cdots,2|-2$，4 不整除 2，所以 x^n-2 为质式。又如：$x^4-2x^3-4x-10$ 也是质式。

容易证明：$f(x)$ 可约 $\Leftrightarrow f(x+b)$ 可约。

例如，设 p 是质数，则 $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ 是质式。

证明：令 $t=x-1$，则 $x=t+1$，代入 $f(x)$ 得

$$\begin{aligned} f(x) &= (x^p-1)/(x-1) \\ &= ((t+1)^p-1)/t \\ &= (t^p + pt^{p-1} + \cdots + pt)/t \\ &= t^{p-1} + pt^{p-2} + \cdots + p \end{aligned}$$

因为存在质数 p，p 不整除 1，而 p 整除后面的所有系数，且 p^2 不整除 p，所以是质式。

若整系数多项式 $f(x)$ 在有理数域上不可约，是否一定能找到一个整数 b，和一质数 p，使 $g(y)=f(y+b)$，满足 Eisenstein 定则的条件呢？答案是不一定。

例如，$f(x)=x^2+2x+5$ 是质式，令

$$g(y) = y^2 + 2(b+1)y + 2b + 5 + b^2$$

设存在质数 p，使得

$$p|2(b+1) \qquad (1)$$

$$p|2b+5+b^2 \qquad (2)$$

$$P^2 \text{ 不整除 } 2b+5+b^2 \qquad (3)$$

若 p 为奇质数，由(1) 有

$$p|b+1$$

再由(2)有

$$\begin{aligned} b+1 &= ps \\ b^2+2b+5 &= pr \end{aligned}$$

所以

$$\begin{aligned} (ps-1)^2 + 2(ps-1) + 5 &= pr \\ p^2s^2 + 4 &= pr \\ r - ps^2 &= 4/p \end{aligned}$$

上式左边是整数，右边是分数，矛盾。

若 $p=2$，则由(2)，b^2 必须为奇数。所以 b 为奇数，设 $b=2m+1$，则

$$\begin{aligned} b^2+2b+5 &= 4m^2+4m+1+4m+2+5 \\ &= 4(m^2+2m+2) \end{aligned}$$

所以 $p^2|b^2+2b+5$，与(3)矛盾。总之，定理 3 充分但不必要。

例如，证明 $f(x)=x^5-x^2+1$ 不可约。

证明：若 $f(x)$ 在 R_0 上可约，则此式两边对质数 p 取模，便知在 R_p 上可约，因此若 $f(x)$ 在 R_p 上不可约，则在 R_0 上必不可约(R_p 上可约，在 R_0 上不一定)。现在模 2 中看，则 $f(x)=x^5-x^2+1$，

(1) 先证无一次因式，R_2 上只有 0,1，分别代入知都不是根，无根，故无一次因式。

(2) 再证无二次因式，在 R_2 上二次因式只有四个，

$$x^2, x^2+x, x^2+1, x^2+x+1$$

不难验证只有 x^2+x+1 是质式，但 $x^5+x^2+1=x^2(x+1)(x^2+x+1)+1$，故无二次因式。

(3)综上也无三次以上因式。

所以 x^5-x^2+1 不可约。

由定理 3，我们立即可得

定理 4 对任意 $n\geq1$，有理域上有 n 次质式。

下面我们讨论求有理数多项式的有理根问题。由于任意有理数多项式和一个整系数多项式相通。所以可以限于讨论求整系数多项式的有理根问题。

定理 5 设

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$$

是整系数多项式。若有理数 b/c 是 $f(x)$ 的根，其中 b 和 c 是互质的整数，则

$$b|a_n, c|a_0.$$

证明：因为 b/c 是 $f(x)$ 的根，所以 $(x-b/c)|f(x)$，所以 $(cx-b)|f(x)$，因 c,b 互质，所以 $cx-b$ 是本原多项式，故商应是整系数多项式。所以，

$$f(x)=(cx-b)(d_0x^{n-1}+\cdots+d_{n-1})$$

比较两边的首系数和常数项得：

$$a_0=cd_0 \qquad a_n=-bd_{n-1},$$

故定理得证。

由定理 5，可得求有理根的方法：

(1) 分别找 a_0,a_n 的所有因子 c_i,b_j；

(2) 找互质对 (c_i,b_j)；

(3) 判断 b_i/c_j 是否为根；

(4) 判断重根。

有理系数多项式除了有理根外其余的根当然是无理数和虚数。

定义 复数 α 称为一个代数数，如果 α 是某个有理系数非 0 多项式的根。若 α 不是任何有理系数非 0 多项式的根，则 α 称为一个超越数。

可以证明圆周率 $\pi=3.141592\cdots$ 和自然对数底 $e=2.71828\cdots$ 都是超越数。一些有理数通过有限次加减乘除及开整数次方得到的数都是代数数，但在 *Galois* 理论中可以证明并不是任意代数数可以这样表示。

习 题

1. 求下列多项式的有理根：
   1) $x^3-6x^2+15x-14$；
   2) $4x^4-7x^2-5x-1$；
   3) $x^5+x^4-6x^3-14x^2-11x-3$。
2. 编一个程序求有理系数多项式的有理根。
3. 求证 x^3-3x+1 在 R_0 上不可约。

4. 求证 x^5+3x^2-1 在 R_0 上不可约。提示：证明此式在 R_2 上不可约。

5. 求证 $x^4+3x^3+3x^2-5$ 在 R_0 上不可约。提示：在 R_2 上分解此式，若在 R_0 上可约，必可分出一次因式。

6. 试用 Eisenstein 定则证明多项式

$$(x^p-1)/(x-1)$$

在 R_0 上不可约，其中 p 是质数。提示：作代换 $t=x-1$ 将此式变为 t 的多项式。

7. 证明代数数只有可数无穷多个，从而断定超越数有不可数无穷多个。

§5 分圆多项式

现在我们首先在复数域中讨论一些结论。

定义 复数域上方程 $x^n-1=0$ 的 n 个根称为 n 次单位根，即 1 的 n 个 n 次方根，根据复数域上多项式可分解为一次质式乘积，知其存在。

例如，$x^2-1=0$ 的根是 ±1，故 $1,-1$ 是二次单位根；

$x^3-1=0,(x-1)(x^2+x+1)=0$，所以 1 是三次单位根；

$x^4-1=0,(x^2+1)(x^2-1)=0$，所以 $x=1,-1,\pm\sqrt{-1}$ 是四次单位根。

下面我们讨论如何求 n 次单位根，我们采用复数的极坐标来表示，则有下面几点性质：

(1) $a+bi$ 表示为 $r(\cos\theta+i\sin\theta)$

(2) $r(\cos\theta+\sin\theta)s(\cos\varphi+i\sin\varphi)$

$=rs[\cos(\theta+\varphi)+i\sin(\theta+\varphi)]$

(3) $[r(\cos\theta+i\sin\theta)]^n=r^n(\cos n\theta+i\sin n\theta)$

设方程 $x^n-1=0$ 的根为 $x=r(\cos\theta+i\sin\theta)$，则 $x^n=r^n(\cos n\theta+i\sin n\theta)$，所以

$$r^n(\cos n\theta+i\sin n\theta)=(\cos 0+i\sin 0)$$
$$=(\cos(2k\pi)+i\sin(2k\pi))$$

所以 $r^n=1,n\theta=2k\pi$，即 $r=1,\theta=(2k\pi)/n$，于是

$$x=\cos(2k\pi/n)+i\sin(2k\pi/n),k=0,\cdots,n-1,$$

为 n 个不同的根。令

$$\xi=\cos(2\pi/n)+i\sin(2\pi/n)$$

则可以看出这 n 个不同的根是 $1,\xi,\cdots,\xi^{n-1}$，这 n 个根的模均是 1，幅角依次相差 $2\pi/n$，故在平面上，恰好将单位圆圆周 n 等分。

例如，$n=5$，则 5 个 5 次方根分别是

$1=\cos 0+i\sin 0,\cos(2\pi/5)+i\sin(2\pi/5),\cos(4\pi/5)+i\sin(4\pi/5),\cos(6\pi/5)+i\sin(6\pi/5),$ $\cos(8\pi/5)-i\sin(8\pi/5)$。

定理 1 复数域中恰有 n 个 n 次单位根，它们在乘法下作成一个 n 元循环群，ξ 是一个生成元素。

证明：根据上面的讨论，n 个 n 次单位根可记做 $1,\xi,\xi^2,\cdots,\xi^{n-1}$，这恰好做成 n 元循环群，ξ 是一个生成元素。

例如，四次单位根 $1,-1,i,-i$ 是乘法循环群。i 是一个生成元素，

$$i=\cos(\pi/2)+i\sin(\pi/2)$$
$$i^2=\cos\pi+i\sin\pi=-1$$

$$i^3 = \cos(3\pi/2) + i\sin(3\pi/2) = -i$$

定义 n 次单位根乘法循环群的生成元素叫本原 n 次单位根。

我们知道，n 元循环群共有 $\varphi(n)$ 个生成元素，所以，共有 $\varphi(n)$ 个本原 n 次单位根，设为

$$\xi_1, \xi_2, \cdots, \xi_{\varphi(n)},$$

例如，二次本原单位根有 $\varphi(2)=1$ 个，-1 是，1 不是。

三次本原单位根有 $\varphi(3)=2$，$\frac{-1+\sqrt{-3}}{2}$，$\frac{-1-\sqrt{-3}}{2}$是，1 不是。

四次本原单位根有 $\varphi(4)=2$，i，$-i$ 是，1，-1 不是。

定义 令 $\Phi_n(x)=(x-\xi_1)(x-\xi_2)\cdots(x-\xi_{\varphi(n)})$。$\Phi_n(x)$称为分圆多项式，意思是说求出它的一个根就可以把单位圆分成 n 等份了。显然，$\Phi_n(x)$的次数是 $\varphi(n)$。

例如，求 $\Phi_1(x)$，应找 $x-1$ 的本原根 1，即 $\Phi_1(x)=x-1$；

$$\Phi_2(x)=x+1 \quad （本原根为 -1）;$$

$$\Phi_3(x)=\left(x-\frac{-1+\sqrt{-3}}{2}\right)\left(x-\frac{-1-\sqrt{-3}}{2}\right)$$

$$=x^2+x+1;$$

$$\Phi_4(x)=(x+i)(x-i)=x^2+1$$

$$\Phi_5(x)=x^4+x^3+x^2+x+1。$$

定理 2 我们有下列公式成立：

$$x^n-1=\prod_{d|n}\Phi_d(x)$$

证明：设 $\theta_1, \theta_2, \cdots, \theta_n$ 是所有 n 次单位根，于是

$$x^n-1=(x-\theta_1)(x-\theta_2)\cdots(x-\theta_n) \tag{1}$$

先证 $\Phi_d(x)|x^n-1$，其中 $d|n$

取一个 $d|n$，设 θ 是一个本原 d 次单位根，于是，$\theta^d=1$，所以，$\theta^n=1$，所有 $\varphi(d)$ 个本原 d 次单位根都出现在 $\theta_1, \cdots, \theta_n$ 中，它们所对应的一次式之积便是 $\Phi_d(x)$，所以，$\Phi_d(x)|x^n-1$。

再证 $\prod_{d|n}\Phi_d(x)|x^n-1$

若 $d\neq d'$，因为 $\Phi_d(x)$ 与 $\Phi_{d'}(x)$的根分别为本原 d 次单位根和本原 d' 次单位根，所以 $\Phi_d(x)$与 $\Phi_{d'}(x)$无公因式，故 $\prod_{d|n}\Phi_d(x)|x^n-1$。

最后证(1)式中任意一因子 $x-\theta_i$ 必在某 $\Phi_d(x)$中出现。

因 $\theta_i^n=1$，故必存在一周期 $t|n$，使得 $\theta_i^t=1$，这样 θ_i 是本原 t 次单位根，故 $x-\theta_i$ 必在某个 $\Phi_d(x)$中出现，其中，$d|n$，故 $x^n-1|\prod_{d|n}\Phi_d(x)$；

综上定理成立。

例如，$x^4-1=\Phi_1(x)\Phi_2(x)\Phi_4(x)$

$$=(x^2+1)(x+1)(x-1)$$

在四个 4 次单位根 1、-1，i、$-i$ 中，i、$-i$ 是本原 4 次单位根，-1 是本原 2 次单位根，1 是本原 1 次单位根。

例如，$\Phi_6(x)=(x^6-1)/(\Phi_1(x)\Phi_2(x)\Phi_3(x))$

$$=(x^6-1)/((x-1)(x+1)(x^2+x+1))$$

$$=x^2-x+1$$

$\Phi_7(x)=x^6+\cdots+1$　（习题 2）

$\Phi_8(x)=x^4+1$　（习题 3）

$\Phi_9(x)=x^6+x^3+1$　（习题 3）

$\Phi_{10}(x)=(x^{10}-1)/(\Phi_5(x)\Phi_2(x)\Phi_1(x))$

因为 $x^5-1=\Phi_5(x)\Phi_1(x)$

所以 $\Phi_{10}(x)=(x^{10}-1)/((x^5-1)\Phi_2(x))$

$=(x^5+1)/(x+1)$

$=x^4-x^3+x^2-x+1$

$\Phi_{11}(x)=x^{10}+\cdots+1$　（习题 2）

$\Phi_{12}(x)=(x^{12}-1)/(\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x))$

因为 $x^6-1=\Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x)$

所以 $\Phi_{12}(x)=(x^{12}-1)/((x^6-1)\Phi_4(x))$

$=(x^6+1)/(x^2+1)$

$=x^4-x^2+1$

定理 3　$\Phi_n(x)$是整系数多项式。

证明：用数学归纳法。

$\Phi_1(x)=x-1$ 是整系数多项式，

设当 $k<n$ 时，$\Phi_k(x)$是整系数多项式，试证 $\Phi_n(x)$亦对。

由定理 2 知，$x^n-1=\Phi_n(x)\prod\limits_{\substack{d\mid n\\ d<n}}\Phi_d(x)$

根据归纳假设，$\prod\limits_{\substack{d\mid n\\ d<n}}\Phi_d(x)$ 是整系数多项式且首系数为 1。

根据上节定理 2，$(x^n-1)/\prod\limits_{\substack{d\mid n\\ d<n}}\Phi_d(x)$ 是整系数多项式。

所以 $\Phi_n(x)$是整系数多项式。

下面我们看任意域 F，设 n 不是其特征的倍数

若在 F 中有根，域 F 中的 n 次单位根仍定义为 $x^n-1=0$ 的根。这里回避了根存在的问题。复数域中代数基本定理等保证其有根；在任意域 F 中，可以证明：对任意域 F 上的 n 次多项式 $f(x)$ 存在域 $K\supseteq F$，使在 K 中 $f(x)$恰有 n 个根，即 K 中 $f(x)$完全分解为一次因式。

因为 n 不是特征倍数，则微商 nx^{n-1}不为零，而 nx^{n-1}只能有根 0，而 0 不是 x^n-1 的根，故 nx^{n-1}与 x^n-1 无公共根，根据§3 定理 5，x^n-1 无重根。

分圆多项式 $\Phi_n(x)$是整系数多项式，把系数当成 F 中元素而看做域 F 上的多项式，这就唯一确定了域 F 上的第 n 个分圆多项式。$x^n-1=\prod\limits_{d\mid n}\Phi_d(x)$ 式是整系数多项式之间的一个等式，因而在 $F[x]$中仍能成立。

定理 4　设 n 不是 F 的特征的倍数，并设 $\Phi_n(x)$在 F 中有根，于是，F 中恰有 n 个 n 次单位根，它们在乘法下作成一个 n 元循环群，其中 $\varphi(n)$个生成元素恰是 $\Phi_n(x)$的所有的根。

证明：设 ξ 是 $\Phi_n(x)$在 F 中的任意根，下面证 ξ 的周期为 n。由于 $\Phi_n(x)\mid x^n-1$，ξ 是 x^n-1 的根，因而 $\xi^n=1$，设 ξ 的周期为 k，则 $k\mid n$，假定 $k<n$，因为 $\xi^k=1$，所以 ξ 应是 x^k-1 的根。但

$$x^k-1=\prod_{d\mid k}\Phi_d(x)$$

此式右边没有$\Phi_n(x)$，而ξ既是x^n-1的根又是$\Phi_n(x)$的根，所以是x^n-1的重根，矛盾，所以ξ的周期为n。所以$1,\xi,\xi^2,\cdots,\xi^{n-1}$是$n$个不同的$n$次单位根，但$x^n-1$最多只能有$n$个根，所以$F$中恰有$n$个$n$次单位根，因$\xi$的周期为$n$，所以在乘法下作成一个$n$元循环群，且$\Phi_n(x)$的任意根$\xi$是此群的一个生成元素，今$n$元循环群只有$\varphi(n)$个生成元素，所以$\Phi_n(x)$的根恰是所有的生成元素。

此n元循环群的生成元素也象在整数域中一样叫本原n次单位根。

注意复数域中用n次单位根乘法循环群$\varphi(n)$个生成元素定义$\Phi_n(x)$，然后证是整数，现在反过来，因整系数而在域F中有意义，再来证它的$\varphi(n)$个根如果存在，仍是x^n-1的n次单位根乘法循环群的生成元素。

例如，在$R_2=\{0,1\}$上看$x^3-1=0$的根，$x^3-1=(x-1)(x^2+x+1)$，而x^2+x+1是质式，故x^3-1在R_2中只有一个根，没有三个三次单位根。现在找域$K\supseteq R_2$使K中有三个三次单位根，引入记号α，希望它是x^3-1的根，且$\alpha\neq1$。因为$\alpha^3-1=0$，即$(\alpha-1)(\alpha^2+\alpha+1)=0$，但$\alpha\neq1$，所以$\alpha^2+\alpha+1=0$，做出$K$如下：

$$K=\{0,1,\alpha,\alpha^2\}$$

K中乘加如下

+	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

·	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

于是x^3-1在K中有三个根$1,\alpha,\alpha^2$

习　　题

1. 求$\Phi_{72}(x)$
2. P是质数时，求$\Phi_P(x)$。
3. P是质数时，求$\Phi_{P^2}(x)$。
4. θ是n次单位根时，证明

$$1+\theta+\theta^2+\cdots+\theta^{n-1}=\begin{cases}n, & 当\ \theta=1\\ 0, & 当\ \theta\neq1\end{cases}$$

5. 设m和n互质，

$$\alpha_1,\alpha_2,\cdots,\alpha_m$$

是所有m次单位根，

$$\beta_1,\beta_2,\cdots,\beta_n$$

是所有n次单位根，求证：

$$\alpha_i\beta_j,i=1,\cdots,m,j=1,\cdots,n$$

便是所有mn次单位根。

6. 说明任意复数$\alpha\neq0$恰有n个n次方根，若$\sqrt[n]{\alpha}$代表α的一个n次方根，其余的n次方

根是哪些?

7. 本节中研究 n 次单位根时假定 F 的特征不整除 n。没有这个假定时怎样?

§6 有　限　域

定义　只有有限个元素的域称为有限域,或 Galois 域。

命题　有限域其特征必是质数 p。

证明:若不然,特征为 0,将包含 R_0 为最小子域,但 R_0 元素无限多,矛盾于有限域定义。

引理　有限域 F,元数 q,则其中 $q-1$ 个非零元素适合方程 $x^{q-1}-1=0$,全部 q 个元素适合方程 $x^q-x=0$。

证明:看域 F 中 $q-1$ 个非零元做成的乘法群,其中任意元 a 适合 $a^{q-1}=1$,即适合方程 $x^{q-1}=1$,移项即是 $x^{q-1}-1=0$(在群中可说任意元适合 $x^n=1$ 不能移项得 $x^n-1=0$)。将 $x^{q-1}-1=0$ 两边乘 x,得 $x^q-x=0$,则 $q-1$ 个非零元仍适合,而零也适合。

定理 1　有限域 F,元数 q,则 $q-1$ 个非零元是所有 $q-1$ 次单位根,所有元是 $x^q-x=0$ 的根。

证明:引理已证是 $q-1$ 次单位根,还须证是"全部",因 $x^{q-1}-1=0$ 是 $q-1$ 次,根据 §3 定理 2,最多有 $q-1$ 个根,故它们是全部的 $q-1$ 次单位根。同理 F 的所有元素恰是 x^q-x 的所有的根。

例如,$K=GF(2^2)=\{0,1,\alpha,\alpha^2\}$,元数是 4。其中 3 个非零元是 $x^3-1=0$ 的根,且恰为全部三个三次单位根,所有元适合 $x^4-x=0$。

又如,$R_5=\{0,1,2,3,4\}$

x:1,2,3,4

x^2:1,4,4,1

x^4:1,1,1,1

其中 4 个非零元是 $x^4-1=0$ 的根且是全部四个四次单位根,所有元适合 $x^5-x=0$。

定理 2　F 的 $q-1$ 个非 0 元素在乘法下作成一个 $q-1$ 元循环群,其 $\varphi(q-1)$ 个生成元素恰是 $\Phi_{q-1}(x)$ 的所有的根。

证明:(引用上节定理 4,取定理 4 中 n 是 $q-1$)

先说明 $q-1$ 不是 p 的倍数。

若不然 $p|q-1$,这时 $f(x)=x^{q-1}-1$ 的微商 $f'(x)=0$,于是 $f(x)$ 的所有根就是 $f'(x)$ 的根,从而是公共根。(根据 §3 定理 5)这些根都是重根,但定理 1 证明中已说明这些根是 F 中非零不同元素,不是重根,所以 p 不整除 $q-1$。

再说明 $\Phi_{q-1}(x)$ 在 F 中有根。

因 $x^{q-1}-1=\prod_{d|q-1}\Phi_d(x)=\Phi_{q-1}(x)\cdots\Phi_1(x)$

左边在 F 上有 $q-1$ 根,而这 $q-1$ 个根分别是右边各 $\Phi_d(x)$ 的根,其中 $\Phi_{q-1}(x)$ 有 $\varphi(q-1)$ 个,故有根,所以定理 2 得证。

这是关于有限域的重要结果,证明方法有不同形式,这里是用前节定理 4 证明的,定理 4 说 n 次单位根群是循环群,而本节定理 1 说有限域乘法群是单位根群。

例如,$K=GF(2^2)=\{0,1,\alpha,\alpha^2\}$ 的非零元的集合 $\{1,\alpha,\alpha^2\}$ 是循环群,生成元 α,α^2 是 $\Phi_3(x)$

$=x^2+x+1$ 的根。

又如，$R_5=\{0,1,2,3,4\}$，$\{1,2,3,4\}$是循环群，2 是一个生成元，因为 $2^1=2$，$2^2=4$，$2^3=3$，$2^4=1$，另一个生成元是 3，它们都是 $\Phi_4(x)=x^2+1$ 的根。

以下讨论有限域的构造。

设 F 是有限域，元数 q，特征质数 p，于是有最小域 $R_p\subseteq F$，将 $\Phi_{q-1}(x)$看做 R_p 上的多项式，设它的一个不可约因式是 $\Psi(x)$，次 $\Psi(x)=n$，因为 $x^{q-1}-1=\Phi_{q-1}(x)\cdots\Phi_1(x)=\Psi(x)\cdots$，左边有 $q-1$ 个单位根，右边 $\Psi(x)$分到 n 个，所以 $\Psi(x)$有 n 个根都在 F 内。取 $\Psi(x)$的一个根 ξ，因 $\Phi_{q-1}(x)=\Psi(x)\cdots$，定理 2 已证 $\Phi_{q-1}(x)$的根都是本原的，ξ 是 $\Psi(x)$的根，当然也是 $\Phi_{q-1}(x)$的根，故 ξ 是一个本原 $q-1$ 次单位根。规定 $\sigma(f(x))=f(\xi)$是 $R_p[x]$到 F 的映射。$R_p[x]$是最小域 $R_p\subseteq F$ 上的多项式环，其中元素是多项式，对任 $f(x)\in R_p[x]$，则它在 σ 下的象是 $f(\xi)$。其中由取法知 $\xi\in F$，因此 $f(\xi)$指的是 x 用 ξ 代入，按域 F 中运算求得的值，故 $f(\xi)\in F$。下面验证同态性：

$$\sigma(f(x)+g(x))=f(\xi)+g(\xi)=\sigma(f(x))+\sigma(g(x))$$
$$\sigma(f(x)g(x))=f(\xi)g(\xi)=\sigma(f(x))\sigma(g(x))$$

所以知 σ 是同态映射，且此同态是到 F 上的，事实上，对于 F 中 0，$R_p[x]$有零多项式，则 $\sigma(0)=0$，所以 0 有原象，再看 F 中非零元，因为 ξ 是本原 $q-1$ 次单位根，即是乘法循环群一个生成元，故 F 中任非零元可写成 ξ^k，相应有多项式 $x^k\in R_p[x]$，使得 $\sigma(x^k)=\xi^k$，所以 σ 是 $R_p[x]$到 F 上的同态映射。

下面我们来说明任意域 F 上多项式环 $F[x]$是主理想环，即其中任意理想是主理想。

证明：设 N 是 $F[x]$的任意一个理想，显然，若其中至少二个元素，则 N 中非 0 多项式必有次数最低的，取一个设为 $\rho(x)$，考虑它生成的理想。$(\rho(x))=\rho(x)F[x]$，$\rho(x)F[x]\subseteq N$ 显然，另一方面，对任 $f(x)\in N$，有带余除法 $f(x)=q(x)\rho(x)+r(x)$，次 $r(x)<$次 $\rho(x)$，而 $r(x)=f(x)-q(x)\rho(x)\in N$，而 N 中 $\rho(x)$次数最低，所以只能 $r(x)=0$，这样 $f(x)=q(x)\rho(x)\in\rho(x)F[x]$，所以，$N\subseteq\rho(x)F[x]$，故 $N=\rho(x)F[x]$，即 N 是主理想。从而 $R_p[x]$也是主理想环。

我们已证 σ 是 $R_p[x]$到 F 上的同态映射，则同态核 N 是 $R_p[x]$的一个理想，因而是主理想。设它由 $\rho(x)$生成，则 $N=(\rho(x))=\rho(x)R_p[x]$，按 ξ 取法，知 $\Psi(\xi)=0$，因为 $\sigma(\Psi(x))=\Psi(\xi)=0$，所以，$\Psi(x)\in N$，即 $\rho(x)\mid\Psi(x)$，但 $\Psi(x)$不可约，所以 $\rho(x)$或是常元数或与 $\Psi(x)$相通。若 $\rho(x)$是常元数，则 $R_p[x]$中任意多项式都是它的倍式，就都在核中，于是在 σ 下全为 0，这矛盾于 σ 是到 F 上的同态映射，这表明 $\rho(x)$只能与 $\Psi(x)$相通，所以此同态的核是 $R_p[x]$中主理想 $\Psi(x)R_p[x]$。因此

$$F\cong R_p[x]/(\Psi(x)R_p[x])$$

从另一角度也可以说明 $R_p[x]/(\Psi(x)R_p[x])$是域，因为 $\Psi(x)$是质式，由§2 习题 5 知，$\Psi(x)R_p[x]$是极大理想。再根据第六章§6 定理 10 知，$R_p[x]/(\Psi(x)R_p[x])$是域。

例如，在 $R_2[x]$中知 $\Phi_3(x)=x^2+x+1$ 是质式，$(x^2+x+1)R_2[x]$是极大理想。则 $R_2[x]/((x^2+x+1)R_2[x])$ 是域，记为 $\overline{F}$。域 $\overline{F}$ 中元素是 $R_2[x]$中多项式，按$(x^2+x+1)R_2[x]$划分的剩余类有多少个呢？可看模 x^2+x+1 有多少不同代表元，即看任意 $R_2[x]$中多项式用 x^2+x+1 除所得余式，因余式次数<2，知余式只是 $0,1,x,1+x$，故有四个剩余类，其中运算可通过代表元运算求出，如：

$$\overline{x}+\overline{x+1}=\overline{x+x+1}=\overline{1}$$
$$\overline{x}(\overline{x+1})=\overline{x^2+x}=\overline{1}$$

$$\bar{x}\,\bar{x} = \overline{x^2} = \overline{x+1}$$

对比前面曾举的例子，$K=GF(2^2)=\{0,1,\alpha,\alpha^2\}$可见对应 $0\leftrightarrow\bar{0},1\leftrightarrow\bar{1},\alpha\leftrightarrow\bar{x},\alpha^2\leftrightarrow\overline{x+1}$是同构的，此域也是 $GF(2^2)$。

一般地，如果 $\Psi(x)$是 $R_p[x]$中质式，次 $\Psi(x)=n$，剩余类域 F 中代表元可取所有低于 n 次多项式，即形为 $a_0+a_1x+\cdots+a_{n-1}x^{n-1}$，其中 $a_i\in R_p$，每个 a_i 有 p 种取法，故共有这样多项式 p^n 个，而任意有限域同构于这种域，所以任意域元数为 p^n。

下面我们来证明：特征质数 p 的有限域 F 中任意元素可唯一表为如下形状：

$$a_0+a_1\xi+a_2\xi^2+\cdots+a_{n-1}\xi^{n-1}, \text{其中 } a_0,a_1,\cdots,a_{n-1}\in R_p$$

证明：(1) 先证能表示

F 中的 0 能表示，只须取 $a_0=a_1=\cdots=a_{n-1}=0$ 即可；

现在看 $\alpha\in F,\alpha\neq 0$，因为 $\alpha=\xi^k$，可看做 $f(x)=x^k$ 以 ξ 代入的值 $f(\xi)$，以 $\Psi(x)$除 $f(x)$可有带余除法，

$$f(x)=q(x)\Psi(x)+r(x), \text{次 } r(x)<\text{次 } \Psi(x)=n,$$

以 ξ 代入得 $f(\xi)=r(\xi)$，现对任 $\alpha=\xi^k=f(\xi)=r(\xi)$，已是要求形状，能表示得证。

(2) 证表法唯一

设 $s(x)\in R_p[x]$，次 $s(x)<n$，而有 $s(\xi)=r(\xi)$，需证明 $s(x)=r(x)$。

因 $r(\xi)-s(\xi)=0$ 根据 σ 的定义知：

$$\sigma(r(x)-s(x))=r(\xi)-s(\xi)=0,$$

故 $r(x)-s(x)$在 σ 的核 $\Psi(x)R_p[x]$中，故 $\Psi(x)\mid(r(x)-s(x))$，但次 $\Psi(x)=n>$次$(r(x)-s(x))$，故只能 $r(x)-s(x)=0$，所以 $s(x)=r(x)$。

例如，有限域 $GF(2^2)=\{0,1,\alpha,\alpha^2\}$中，$\alpha$ 是 $\Phi_3(x)$在 $R_2[x]$中不可约因式 x^2+x+1 的根。域中所有元可表成：

$$0+0\alpha=0$$
$$0+1\alpha=\alpha$$
$$1+0\alpha=1$$
$$1+1\alpha=1+\alpha=\alpha^2$$

由上面的讨论知，F 中所有元无遗漏无重复地表成：

$$a_0+a_1\xi+\cdots+a_{n-1}\xi^{n-1}$$

系数取自于 R_p 中 p 个元素，每个位置有 p 种取法，n 个位置共 p^n 种取法。正对应 F 中所有元，所以，特征质数 P 的有限域元数必是 p^n。

定理 3 有限域的元数必为 p^n 的形式，其中 p 为其特征，如果同构的域看作是一样的，则对任意 $q=p^n$ 恰有一个 q 元有限域。

证明：前一句话已证。后一句话有两层含意(1)存在性；(2)唯一性。

先证唯一性。

设 F，F' 是两个 $q=p^n$ 元有限域，它们都包含 R_p 为其子域，都取 $R_p[x]$中的 $\Phi_{q-1}(x)$的不可约因式 $\Psi(x)$，从而都同构于 $R_p[x]/(\Psi(x)R_p[x])$，所以，$F\cong F'$。

再证存在性。

对任给质数 p，正整数 n，设 $q=p^n$，我们来证明 q 元域存在。显然最小域 $R_p=\{0,1,\cdots,p-1\}$存在，将 $\Phi_{q-1}(x)$看做 $R_p[x]$中多项式，设它的一个不可约因式是 $\Psi(x)$，根据§2 习题 5，Ψ

$(x)R_p[x]$是极大理想，根据第六章§6定理10，$R_p[x]/(\Psi(x)R_p[x])$是域，记为$\bar{F}$。

(1) 证$\bar{F}$的特征是质数p，需证明$\bar{1}$的加法周期为p，很显然，因为$R_p[x]$中p个1相加为0，少于p个1相加必不为0，所以对应的$\bar{F}$中的p个$\bar{1}$相加是$\bar{0}$，少于p个$\bar{1}$相加必不为$\bar{0}$，因此，$\bar{F}$的特征是P。

(2) 再证$\bar{F}$中有$q-1$个$q-1$次单位根，想利用上节定理4。已知有域$\bar{F}$，定理4中n取$q-1$，对照条件，先说$q-1$不是p的倍数，显然，因为$q-1=p^n-1$不为p倍数。下面应说明$\Phi_{q-1}(x)$在$\bar{F}$中有根，只须说明$\bar{x}$是一个即可。$\bar{x}$指x所在的剩余类。看$\Psi(\bar{x})$，它表示$\bar{x}$按$\bar{F}$中的加乘进行运算，结果仍是一个剩余类。根据剩余类运算知，结果应是$\Psi(x)$所在的剩余类$\overline{\Psi(x)}$。即$\Psi(\bar{x})=\overline{\Psi(x)}$。再说明按$\Psi(x)R_p[x]$划分剩余类，$\Psi(x)$与0在同一个剩余类。事实上，它们都在理想$\Psi(x)R_p[x]$中，故$\overline{\Psi(x)}=\bar{0}$。这样$\Psi(\bar{x})=\overline{\Psi(x)}=\bar{0}$，这表明在$\bar{F}$中看，$\bar{x}$是$\Psi(x)$的根，因此是$\Phi_{q-1}(x)$的根。所以前节定理4的条件满足，所以$\bar{F}$中恰有$q-1$个$q-1$次单位根，是$\bar{F}$中$q-1$个剩余类。取$\bar{F}$中$q-1$个$q-1$次单位根再加上$\bar{0}$，得$F$，显然$F$元数$q=p^n$，其中加乘运算与在$\bar{F}$中相同，下面验证$F$是域，现在$F$中元满足方程$x^q-x=0$，反过来$x^q-x=0$最多有$q$个根，故$x^q=x$是$F$中元的标志，先证是加子群，任取$\alpha\in F$，$\beta\in F$，则有$\alpha^q=\alpha$，$\beta^q=\beta$，

$$
\begin{aligned}
(\alpha-\beta)^q &= (\alpha-\beta)^{p^n} \\
&= \alpha^{p^n} - \beta^{p^n} \\
&= \alpha^q - \beta^q \\
&= \alpha - \beta
\end{aligned}
$$

所以$\alpha-\beta\in F$。

再证非零元是乘法子群，$\beta\neq 0$时

$$(\alpha/\beta)^q = \alpha^q/\beta^q = \alpha/\beta$$

所以$\alpha/\beta\in F$。

故F是$q=p^n$元域。证毕。

今后把唯一确定的p^n元有限域记为$GF(p^n)$。

定理4 $\Phi_{p^m-1}(x)$在$R_p[x]$中质式$\Psi(x)$为m次，$m\geqslant 1$，所以R_p上有m次质式。

证明：现在已知质数p，正整数m，根据定理3，唯一存在有限域$GF(p^m)$，记为F，其特征为p，对这个F，找$\Psi(x)$是Φ_{p^m-1}的质因式，前面已设次$\Psi(x)=n$，并且推出F中的元数是p^n，而F的元数已知是P^m，从而$n=m$。

例如，问$\Phi_7(x)$在$R_2[x]$中质因式是多少次？

解：因为$7=2^3-1$，所以是3次的。即$\Phi_7(x)=(x^3+x^2+1)(x^3+x+1)$

又如，试求一个R_2上的4次质式。

解：$2^4-1=15$，故$\Phi_{15}(x)$的质因式使是。即$\Phi_{15}(x)=(x^4+x^3+1)(x^4+x+1)$

引理 $t^m-1\mid t^n-1\Leftrightarrow m\mid n$。$t$是一个文字或是一个大于1的整数，$m$，$n$是正整数。

证明：设$n=sm+r$，$0\leqslant r<m$，于是

$$
\begin{aligned}
t^{n-1} &= t^{sm+r} - 1 \\
&= t^{sm+r} - t^r + t^r - 1 \\
&= t^r(t^{sm}-1) + (t^r-1) \\
&= t^r(t^m-1)(t^{sm-m}+t^{sm-2m}+\cdots+1) + (t^r-1)
\end{aligned}
$$

(⇐)若 $m|n$,则 $r=0, t^r-1=0$,上式表明 $t^m-1|t^n-1$。

(⇒)若不然,m 不整除 $n, r\neq 0, t^r-1\neq 0$,

若 t 是大于 1 的整数,则 $t^r-1<t^m-1$;

若 t 是文字,次$(t^r-1)=r<$次$(t^m-1)=m$

所以 t^r-1 是非 0 余数。所以根据上式得 t^m-1 不整除 t^n-1,矛盾。

例如,$2^8-1|2^{24}-1, 2^8-1$ 不整除 $2^{25}-1$。

定理 5　对任意 $m|n$,$GF(p^n)$恰有一个子域 $GF(p^m)$,而这也就是 $GF(p^n)$的所有子域。

证明:先证 $GF(p^n)$有唯一子域 $GF(p^m)$。

因为 $m|n$,所以 $p^m-1|p^n-1$,所以 $x^{p^m-1}-1|x^{p^n-1}-1$,$GF(p^n)$的所有非零元是 $x^{p^n-1}-1$ 的所有根,故其中包含 $x^{p^m-1}-1$ 的所有根,如同定理 3 证明,取出 $x^{p^m-1}-1$ 的所有根,再加上 0,便得 $GF(P^m)$且由定理 3 知,唯一存在一个域 $GF(P^m)$。

再证是所有子域。

设 F 是 $GF(p^n)$的任意子域,其特征当然是 p,因而是 $GF(p^m)$的形式。因为 $GF(p^m)$的非零元是 $GF(p^n)$的非零元的一部分,故在 $x^{p^n-1}-1$ 的完全因式分解中,$GF(p^m)$的非零元一定都出现,并乘为 $x^{p^m-1}-1$,从而 $x^{p^m-1}-1|x^{p^n-1}-1$,由引理 $p^m-1|p^n-1$,再由引理 $m|n$,可见,F 只能是上述 $GF(p^m)$之一。

例如,问 $GF(32)$中有没有 4 元子域?

解:$32=2^5, 4=2^2$,因为 2 不整除 5,所以没有 4 元子域。

习　题

1. $GF(9)$中的元素可表为 $a+b\varphi$ 的形式,其中 a, b 为 0,1,或-1。试列出其乘法表。

2. 设 $\alpha\in GF(p^n)$,求证以 R_p 中元素为系数的 α 的多项式作成一个子域 $GF(p^m)$,并证明,若 α 的周期为 k,则 m 是适合:

$$p^r \equiv 1 \pmod k$$

的最小的 r。

3. 设 $q=p^m$,定理 4 中说,$\Phi_{q-1}(x)$在 $R_p[x]$中的质因式必是 m 次多项式。举例说明 $x^{q-1}-1$ 在 $R_p[x]$中的质因式除属于 $\Phi_{q-1}(x)$的以外还可能有 m 次的。

4. 设 $q=p^m$,求证 $R_p[x]$中的任意 m 次质式必是 x^q-x 的因式,并证明,x^q-x 在 $R_p[x]$ 中的任意质因式的次数必整除 m。

5. 对任意 $m\geqslant 1$,求证 $GF(p^n)$上必有 m 次质式。

6. 在 $GF(p^n)$中,规定一个变换 σ 如下:

$$\sigma(\alpha) = \alpha^p$$

求证 σ 是 $GF(p^n)$的一个自同构,$1, \sigma, \sigma^2, \cdots, \sigma^{n-1}$是 n 个不同的自同构,而 $GF(p^n)$也只有这些自同构。

第八章 格与布尔代数

§1 引 言

在第一章中我们介绍了关于集合的理论，其中有幂集的概念 $\rho(A)$，在 $\rho(A)$ 中有 $A\cup B$、$A\cap B$ 的概念，且交，并可以看做 $\rho(A)$ 上的两个代数运算，这样 $(\rho(A),\cup,\cap)$ 可看做是一个代数，这就是通常所说的集合代数。

在集合代数中，运算 $\cup$、$\cap$ 满足等幂律，交换律，结合律，分配律，吸收律等。

在第二章中我们介绍了命题逻辑，设 S 是所有命题的集合，于是，逻辑连结词 $\wedge$，$\vee$ 就可以看做是集合 S 上的两个代数运算，因此 $(S,\wedge,\vee)$ 可看做是一个代数，这就是通常所说的命题代数。

在命题代数中，运算 $\wedge$，$\vee$ 也满足等幂律，交换律，结合律，分配律，吸收律等。

如果在集合代数中引进余集的概念，在命题代数中引进否定的概念，则在这两种代数中都有类似的所谓 De Morgan 定律。

从代数的观点出发，我们是否能对一种更为抽象的代数系统进行研究，而这种抽象的代数系统又具有象集合代数，命题代数那样具体的代数系统所具有的一些最本质的性质？回答是肯定的。这种抽象的代数系统就是格(Lattice)和布尔代数(Boolean Algebra)。

格和布尔代数在计算机科学中有着重要的应用。

§2 格的定义

定义 A(半序格) 给出一个部分序集 $(L,\leqslant)$。如果对于任意 $a,b\in L$，L 的子集 $\{a,b\}$ 在 L 中都有一个最大下界(记为 $\inf\{a,b\}$)和一个最小上界(记为 $\sup\{a,b\}$)，则称 $(L,\leqslant)$ 为一个格。

显然，一个序集是一个格。但是，不是所有的部分序集都是格，这可从下面的图 8.2.1 所示的某些部分序集的 Hasse 图中看到。

图(a)是序集，也是格；(b)～(g)是部分序集，也是格；图(h)，(i)是部分序集，但不是格。

例如，$S=\{a,b\}$ $\rho(s)=\{\phi,\{a\},\{b\},\{a,b\}\}$，部分序关系是包含于关系，则 $(\rho(S),\subseteq)$ 是一个格。

Hasse 图是图(b)。

又如，$S_{24}=\{1,2,3,4,6,8,12,24\}$，设 D 是整除关系，则 (S_{24},D) 是格。

Hasse 图是图(g)。

再如，令 G 是一个群，L 是所有子群做成的集合，则 L 关于集合的包含于关系是部分序集，任取 $A,B\in L$，自然 $A\cap B$ 是群且是 $\{A,B\}$ 的最大下界，但 $A\cup B$ 不一定是群，即不一定属于 L。下面我们定义 G 中 A 与 B 生成的子群 C，规定是包含 A 和 B 的最小的子群，包含 A 和 B 的子群存在，例如 G 本身就是一个，A、B 生成的子群就是包含 A、B 的所有子群的交集，于是 A,B 生成的子群 $C\in L$ 是 A、B 的最小上界。所以此 L 是格。

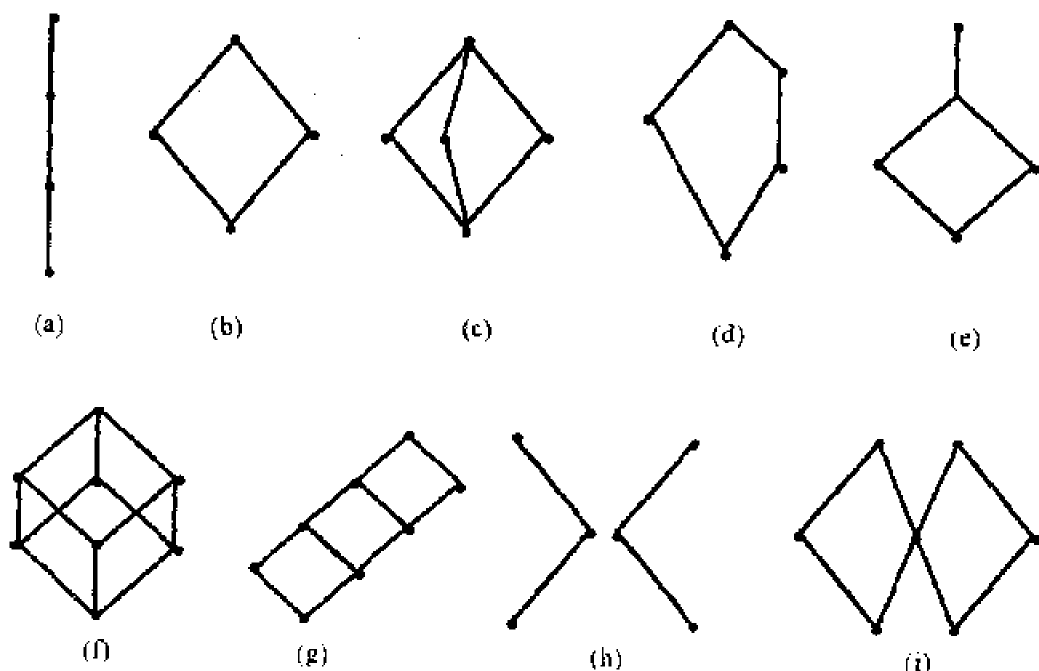


图 8.2.1

定义 A'(半序子格) 设$(L,\leqslant)$是格,S 是 L 的子集,即 $S\subseteq L$,如果$(S,\leqslant)$是格,则称$(S,\leqslant)$是格$(L,\leqslant)$的子格。

例如,(S_6,D)是(S_{24},D)的子格。

定义 B(代数格) 设 L 是一个集合,$\times$,$\oplus$是 L 上两个二元代数运算,如果这两种运算对于 L 中元素满足:

(1) 交换律:$a\times b=b\times a$,$a\oplus b=b\oplus a$;

(2) 结合律:$a\times(b\times c)=(a\times b)\times c$,$a\oplus(b\oplus c)=(a\oplus b)\oplus c$;

(3) 吸收律:$a\times(a\oplus b)=a$,$a\oplus(a\times b)=a$

则称此代数系统$(L,\times,\oplus)$为一个格。

例如,设 S 是一个集合,$\rho(S)$是 S 的幂集合,集合的交、并是 $\rho(S)$上的两个代数运算,于是,$(\rho(s),\cap,\cup)$是一个格。

又如,设 I_+是所有正整数集合,两个正整数的最高公因$\times$,最小公倍$\oplus$可看做是 I_+上两个代数运算,于是,$(I_+,\times,\oplus)$是一个格。

再如,设 n 是一个正整数,S_n 是 n 的所有正因数的集合,两个正整数的最高公因$\times$,最小公倍$\oplus$可看做是 S_n 上两个代数运算,于是,$(S_n,\times,\oplus)$是一个格。

定理 1 定义 A 所定义的格和定义 B 所定义的格是等价的。亦即,一个半序格必是一个代数格;反之亦然。

证明:(1)若$(L,\leqslant)$是一个半序格,规定运算 $a\oplus b=\sup\{a,b\}$,$a\times b=\inf\{a,b\}$。因最小上界和最大下界唯一确定,所以这样规定的$\oplus$,$\times$是 L 上的两种二元代数运算,可以证明$\times$、$\oplus$

满足交换律，结合律，吸收律。我们只证吸收律：

$$a \times (a \oplus b) = a$$

因为 $a\times(a\oplus b)$ 是 a 与 $(a\oplus b)$ 的最大下界，所以 $a\times(a\oplus b)\leqslant a$；另一方面，由于 $a\leqslant a$，$a\leqslant(a\oplus b)$，所以，a 是 a 与 $(a\oplus b)$ 的下界，而 $a\times(a\oplus b)$ 是 a 与 $(a\oplus b)$ 的最大下界，所以 $a\leqslant a\times(a\oplus b)$，所以 $a=a\times(a\oplus b)$。因此，$(L,\times,\oplus)$ 是一个代数格。

(2) 在 L 上定义一个关系 $\leqslant$ 如下：

$$a \leqslant b \Leftrightarrow a \times b = a$$

下面证 $\leqslant$ 是一个部分序关系。

反身性：因为 $a\times a=a\times(a\oplus(a\times a))=a$（吸收律），所以 $a\leqslant a$；

反对称性：若有 $a\leqslant b$，$b\leqslant a$，则应有 $a\times b=a$，$b\times a=b$，而 $a\times b=b\times a$（交换律），所以 $a=b$；

传递性：若 $a\leqslant b$，$b\leqslant a$，则应有 $a\times b=a$，$b\times c=b$，所以 $a\times c=(a\times b)\times c=a\times(b\times c)=a\times b=a$（结合律），所以 $a\leqslant c$。

故 $\leqslant$ 是一个部分序关系。

（我们也可以这样定义 $\leqslant$ 关系，$a\leqslant b\Leftrightarrow a\oplus b=b$）

不难证明：$a\times b=a\Leftrightarrow a\oplus b=b$

($\Rightarrow$) 若 $a\times b=a$，则

$$a \oplus b = (a \times b) \oplus b = b$$

($\Leftarrow$) 若 $a\oplus b=b$，则

$$a \times b = a \times (a \oplus b) = a$$

因此，对任意 $a,b\in L$，

$$a \leqslant b \Leftrightarrow a \oplus b = b$$

下面证在关系 $\leqslant$ 下，任意二元有最大下界就是 $a\times b$，任意二元有最小上界就是 $a\oplus b$。

证明：由吸收律 $a\oplus(a\times b)=a$ ①

$b\oplus(a\times b)=b$ ②

由① $a\times b\leqslant a$，由② $(a\times b)\leqslant b$，所以 $a\times b$ 是 a 与 b 的下界，若又有 c，是 a,b 的下界，即 $c\leqslant a$，$c\leqslant b$，需证 $c\leqslant a\times b$，即需证 $(a\times b)\times c=c$。

因为 $c\times c=c\times(c\oplus(c\times c))=c$，所以 $c\times c=c$，所以

$$\begin{aligned}(a \times b) \times c &= (a \times b) \times (c \times c)\\ &= (a \times c) \times (b \times c)\\ &= c \times c\\ &= c\end{aligned}$$

所以 $a\times b$ 是 a,b 的最大下界。

类似可证：$\sup\{a,b\}=a\oplus b$。

所以，代数格 $(L,\times,\oplus)$ 是一个半序格，证毕。

给出一个半序格 $(L,\leqslant)$，则与其等价的代数格 $(L,\times,\oplus)$ 中，$\times,\oplus$ 分别是半序 $\leqslant$ 下的最大下界和最小上界运算，反之，给出代数格 $(L,\times,\oplus)$ 与其等价的半序格的半序关系是 $a\leqslant b\Leftrightarrow a\times b=a$ 或 $a\oplus b=b$。在证明过程中，我们证出了等幂律，$a\times a=a$，$a\oplus a=a$ 以及 $a\leqslant b\Leftrightarrow a\times b=a\Leftrightarrow a\oplus b=b$。

定义 B'（代数子格） 设 $(L,\times,\oplus)$ 是一个格，S 是 L 的一个子集，$(S,\times,\oplus)$ 称为 $(L,\times,\oplus)$ 的一个子格，当且仅当在运算 $\times,\oplus$ 下，S 是封闭的。

命题　$(S,\times,\oplus)$是代数格$(L,\times,\oplus)$在定义B′意义下的代数子格$\Leftrightarrow S\subseteq L$且$(S,\times,\oplus)$是代数格。

证明：($\Rightarrow$)按定义B′，$S\subseteq L$，$\times$，$\oplus$运算封闭，须说明S中满足定义B'中的三个算律，但因在L中满足，故在S中满足。

($\Leftarrow$)$(S,\times,\oplus)$是代数格，当然要求运算封闭。

例如，$(S_{24},\times,\oplus)$是代数格，与之等价的半序格为(S_{24},D)，$(S_6,\times,\oplus)$是代数子格，(S_6,D)是半序子格。$(\{1,2,3,12\},D)$是半序子格，但不是代数子格。因为$2\oplus3=6$，不封闭。

结论：设$(L,\leqslant)$是一个格，与其等价的代数格是$(L,\times,\oplus)$，S是L的一个子集。

(1) 若$(S,\times,\oplus)$是$(L,\times,\oplus)$的代数子格，则$(S,\leqslant)$是$(L,\leqslant)$的半序子格。

(2) 若$(S,\leqslant)$是$(L,\leqslant)$的半序子格，则$(S,\times,\oplus)$不一定是$(L,\times,\oplus)$的代数子格。

例如，设$(L,\leqslant)$是如图8.2.2的一个格，取$S_1=\{a_1,a_2,a_4,a_6\}$，则$(S_1,\leqslant)$是$(L,\leqslant)$的半序子格，$(S_1,\times,\oplus)$是$(L,\times,\oplus)$的代数子格；但取$S_2=\{a_1,a_2,a_4,a_8\}$，则$(S_2,\leqslant)$仍是$(L,\leqslant)$的半序子格，但$(S_2,\times,\oplus)$不是$(L,\times,\oplus)$的代数子格，因S_2中看a_2,a_4最大下界是a_8，如按此规定$a_2\times a_4=a_8$则与原L中运算不一致，与$(S_2,\leqslant)$等价的代数格中必须$a_2\times a_4=a_8$已不是$(L,\times,\oplus)$的代数子格。一般地，任意代数系统的子系统要求对原系统一切运算封闭。

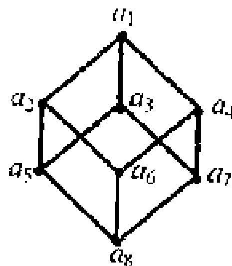


图8.2.2

例如，Klein群G的所有子群做成的格L，设$G=\{e,a,b,c\}$，$L=\{I,H_1,H_2,H_3,G\}$，再看G的所有子集做成的幂集格$(\rho(G),\subseteq)$，就集合的包含于关系来看，L是$\rho(G)$的子集，在包含于关系下，半序格L是$\rho(G)$半序子格；就代数格看，L中与$\rho(G)$中运算不同，所以L不是$\rho(G)$的代数子格。

习　题

1. 设S是所有命题作成的集合，说明S在什么运算下作成代数格，在什么部分序下作成半序格。

2. 设$(L,\times,\oplus)$是一个格，$a,b\in L$。令

$$S=\{x\mid x\in L,a\leqslant x\leqslant b\}$$

其中$\leqslant$是与$(L,\times,\oplus)$等价的半序格中的部分序，证明：$(S,\times,\oplus)$是L的子格。

§3　格的性质

定理1　设$(L,\leqslant)$是一个格，a,b是L中任意元素，于是

$$a\leqslant b\Leftrightarrow a\times b=a$$
$$\Leftrightarrow a\oplus b=b$$

证明：在§2定理1的证明过程可以得到此结论。

定理2　设$(L,\leqslant)$是一个格，a,b,c是L中任意元素，如果$b\leqslant c$，则有

$$a\times b\leqslant a\times c$$
$$a\oplus b\leqslant a\oplus c$$

证明：因为 $b\leqslant c$，所以由定理 1 知

$$b \times c = b$$

又因为

$$\begin{aligned}(a \times b) \times (a \times c) &= (a \times a) \times (b \times c) \\ &= a \times (b \times c) \\ &= a \times b\end{aligned}$$

由定理 1 知：　$a \times b \leqslant a \times c$

同理可证 $a \oplus b \leqslant a \oplus c$

定理 3　设 $(L,\leqslant)$ 是一个格，a,b,c 是 L 中任意元素，于是有

$$a \oplus (b \times c) \leqslant (a \oplus b) \times (a \oplus c)$$

$$(a \times b) \oplus (a \times c) \leqslant a \times (b \oplus c)$$

证明：因为 $a\leqslant a\ominus b, a\leqslant a\oplus c$，所以，由 $\times$ 的定义知

$$a \leqslant (a \ominus b) \times (a \oplus c)$$

又因为

$$b \times c \leqslant b \leqslant a \oplus b$$

$$b \times c \leqslant c \leqslant a \oplus c$$

所以，再由 $\times$ 的定义知

$$b \times c \leqslant (a \oplus b) \times (a \oplus c)$$

所以

$$a \oplus (b \times c) \leqslant (a \oplus b) \times (a \oplus c)$$

同理可证另一不等式。

定理 3 证出 $a\oplus(b\times c)\leqslant(a\oplus b)\times(a\oplus c)$ 成立，但反过来不一定成立。请读者给一反例。这说明在任意格中没有分配律。

定理 4　设 $(L,\leqslant)$ 是一个格，a,b,c 是 L 中任意元素，于是

$$a \leqslant b \Leftrightarrow a \oplus (b \times c) \leqslant b \times (a \ominus c)$$

证明：若 $a\leqslant b$，则由定理 1 知：$a\oplus b=b$，再由定理 3 知

$$\begin{aligned}a \oplus (b \times c) &\leqslant (a \oplus b) \times (a \oplus c) \\ &= b \times (a \oplus c)\end{aligned}$$

反之，若 $a\ominus(b\times c)\leqslant b\times(a\ominus c)$，则由 $\oplus$ 的定义知

$$a \leqslant a \oplus (b \times c)$$

由 $\times$ 的定义知

$$b \times (a \oplus c) \leqslant b$$

所以 $a\leqslant b$。

定义　设 $(L,\times,\oplus)$ 和 $(S,\wedge,\vee)$ 是两个格，L 到 S 内的映射 g 称为 $(L,\times,\ominus)$ 到 $(S,\wedge,\vee)$ 的格同态映射，如果对任意 $a,b\in L$，都有

$$g(a \times b) = g(a) \wedge g(b)$$

$$g(a \oplus b) = g(a) \vee g(b)$$

格 L 到 L 内的同态映射称为格的自同态映射，若 g 是 L 到 S 上的同态映射，且是一对一的，则称 g 是格同构映射，并称格 L 与格 S 是同构的。

显然，格的同构映射 g 必存在其逆映射，g^{-1}，并且对 $x\in L$ $y\in S$ 有

$$g^{-1}(g(x))=x \qquad g(g^{-1}(y))=y。$$

定理 5　设$(L,\times,\oplus)$和$(S,\wedge,\vee)$是两个格，集合 L 上对应于运算$\times$，$\oplus$的部分序为$\leqslant_L$，集合 S 上对应于运算$\wedge$，$\vee$的部分序为$\leqslant_S$，如果 g 是 L 到 S 内的同态映射，则 g 是保序映射。亦即，对任意 $a,b\in L$，若 $a\leqslant_L b$，则 $g(a)\leqslant_S g(b)$。

证明：因为 $a\leqslant_L b\Leftrightarrow a\times b=a$，所以 $g(a\times b)=g(a)$。而

$$\begin{aligned} g(a\times b) &= g(a)\wedge g(b) \\ &= g(a) \end{aligned}$$

故 $g(a)\leqslant_S g(b)$。

本定理的逆定理不成立，即保序不一定同态(习题 5)，若双保序，则同构(习题 9)。

定理 6　设$(L,\times,\oplus)$是一个格，g 是此格的自同态映射，于是 $g(L)$是$(L,\times,\oplus)$的子格(定义 B′)。

证明：任取 $g(L)$中两个元素，a',b'，则必有 $a\in L,b\in L$，使得

$$a'=g(a),b'=g(b)$$

因为 g 是格$(L,\times,\oplus)$的自同态映射(运算一样)，所以

$$a'\times b'=g(a)\times g(b)=g(a\times b)\in g(L)$$
$$a'\oplus b'=g(a)\oplus g(b)=g(a\oplus b)\in g(L)$$

即在运算$\times$，$\oplus$下，$g(L)$是封闭的，故$(g(L),\times,\oplus)$是$(L,\times,\oplus)$的子格。

定理 7　设$(L,\times,\oplus)$，$(S,\wedge,\vee)$是两个格，若 g 是 L 到 S 上的同构映射，则 g 的逆映射 g^{-1}是 S 到 L 上的同构映射。

证明：显然 g^{-1}是 S 到 L 上的一对一映射，以下证 g^{-1}是同态映射即可。

任取 $a',b'\in S$，令 $g^{-1}(a')=a,g^{-1}(b')=b$，于是

$$g(a)=a',g(b)=b'$$

所以

$$\begin{aligned} g^{-1}(a'\wedge b') &= g^{-1}(g(a)\wedge g(b)) \\ &= g^{-1}(g(a\times b)) \\ &= a\times b \\ &= g^{-1}(a')\times g^{-1}(b') \end{aligned}$$

同理可证：$g^{-1}(a'\vee b')=g^{-1}(a')\oplus g^{-1}(b')$。

故 g^{-1}是 S 到 L 上的同构映射。

推论　若格$(L,\times,\oplus)$和格$(S,\wedge,\vee)$同构，g 是其同构映射。则对 L 中任意两个元素 a,b 有

$$a\leqslant_L b\Leftrightarrow g(a)\leqslant_S g(b)$$

其中$\leqslant_L$，$\leqslant_S$ 分别是集合 L,S 上对应于运算$\times$、$\wedge$的部分序关系。

根据定理 5 及定理 7 不难证明此推论。

例如，令 $L=\{0,1\}$，规定 $0\leqslant 1$，则$(L,\leqslant)$是一个格，并且令$(L,\wedge,\vee)$是与之等价的代数格，则$\wedge$，$\vee$分别是集合 L 中两个元素的最大下界、最小上界运算。令

$$L^n=\{(a_1,\cdots,a_n)\mid a_i\in L,i=1,\cdots\cdots,n\}$$

规定：

$$(a_1,\cdots,a_n)\leqslant_n(b_1,\cdots,b_n)\Leftrightarrow a_i\leqslant b_i(i=1,\cdots,n)$$

则不难证明：$(L^n,\leqslant_n)$是一个格，通常称为 n 维格，令与$(L^n,\leqslant_n)$等价的代数格为$(L^n,\times,\oplus)$，

则显然有

$$(a_1,\cdots,a_n)\times(b_1,\cdots,b_n)=(a_1\wedge b_1,\cdots,a_n\wedge b_n)$$

$$(a_1,\cdots,a_n)\oplus(b_1,\cdots,b_n)=(a_1\vee b_1,\cdots,a_n\vee b_n)$$

又如，令 $S=\{s_1,\cdots,s_n\}$，则其幂集合 $(\rho(S),\subseteq)$ 与 $(L^n,\leqslant_n)$ 同构。

证明：规定映射 $g:\rho(s)\leftrightarrow L^n$ 如下：

若 A 是 S 的子集，则 $g(A)=(a_1,\cdots,a_n)$，其中，$a_i=1\Leftrightarrow s_i\in A\ (i=1,\cdots,n)$

(如 $A=\{S_1,S_2\}$ 则 $g(A)=(1,1,0,0,\cdots,0)$)

显然，g 为一对一映射。

任取 $A,B\in\rho(S)$，设 $g(A)=(a_1,\cdots,a_n)$，$g(B)=(b_1,\cdots,b_n)$，$g(A\cap B)=(c_1,\cdots,c_n)$，据 g 的定义：

$$a_i=1\Leftrightarrow s_i\in A$$

$$b_i=1\Leftrightarrow s_i\in B$$

$$c_i=1\Leftrightarrow s_i\in A\cap B$$

所以，

$$c_i=1\Leftrightarrow a_i=1\text{ 同时 }b_i=1,i=1,\cdots,n。$$

因此，$c_i=a_i\wedge b_i$。所以，

$$(c_1,\cdots,c_n)=(a_1,\cdots,a_n)\times(b_1,\cdots,b_n)$$

即，$g(A\cap B)=g(A)\times g(B)$。

同理可证：$g(A\cup B)=g(A)\oplus g(B)$。故 $(\rho(S),\cap,\cup)$ 与 $(L^n,\times,\oplus)$ 同构。

习　题

1. 设 $(L,\leqslant)$ 是格，若 $a,b,c\in L$，$a\leqslant b\leqslant c$，则

$$a\oplus b=b\times c$$

$$(a\times b)\oplus(b\times c)=(a\oplus b)\times(a\oplus c)$$

2. 设 $(L,\leqslant)$ 是格，若 $a\leqslant b$，$c\leqslant d$，$a,b,c,d\in L$，则 $a\times c\leqslant b\times d$，$a\oplus c\leqslant b\oplus d$

3. 设 $(L,\leqslant)$ 是一个格，证明：

$$(a\times b)\oplus(c\times d)\leqslant(a\oplus c)\times(b\oplus d)$$

$$(a\times b)\oplus(b\times c)\oplus(c\times a)\leqslant(a\oplus b)\times(b\oplus c)\times(c\oplus a)$$

4. 若 $(L,\leqslant)$ 是有限格，则 L 中必有最小、最大元素。

5. 举例说明：对于两个格 L 和 S，g 是 L 到 S 的保序映射，但是 g 不是同态映射。

6. 令 $S=\{$所有正偶数集合$\}$，证明：(I_+,D) 与 (S,D) 同构。

7. 证明：4 个元素的格 $(L,\times,\oplus)$ 必同构于格 $(I_4,\leqslant)$ 或者格 (S_6,D)。

8. 证明：格 $(E,\leqslant)$ 和格 $(O,\leqslant)$ 同构，其中 E 是正偶数集，O 是正奇数集，$\leqslant$ 是数的小于等于关系。给出的同构映射是否是格 (E,D) 和格 (O,D) 之间的同构映射？其中 D 是整除关系。

9. 设 $(L,\times,\oplus)$，$(S,\wedge,\vee)$ 是两个格。证明：若 g 是 L 到 S 上的一对一映射，则 g 是同构映射的充要条件是 g 与 g^{-1} 是保序映射。

10. 设 $(L,\times,\oplus)$ 是有限格，g 是 L 到 L 内的映射。如果对任意 $a,b\in L$，有 $g(a\times b)=g(a)\times g(b)$，则必有 $e\in L$，使得 $g(e)=e$。

11. 证明：§3 中定理 7 的推论。

§4　几种特殊的格

我们知道，在一个格里，任意一对元素都有一个最大下界和一个最小上界。我们推广这个事实。

引理 1　设$(L,\leqslant)$是一个格，若 S 是 L 的任意一个有限非空子集，则 S 有一个最大下界和一个最小上界，分别记为 $\inf S$，$\sup S$。

证明：设 $S=\{a_1,\cdots,a_t\}$，则据定义知

$$a_1 \times a_2 \times \cdots \times a_t \text{ 是最大下界}$$

$$a_1 \oplus a_2 \oplus \cdots \oplus a_t \text{ 是最小上界}$$

若 S 是无限的，则不对。如正整数 I_+ 取普通小于等于关系，则$(I_+,\leqslant)$是格，取正偶数集合 E_+ 是无限非空子集，则 E_+ 无上确界，下确界为 2。

定义　格$(L,\leqslant)$称为*有界格*，如果它有一个最大元素（记为 1）和一个最小元素（记为 0），亦即，对任意 $a\in L$，都有 $0\leqslant a\leqslant 1$，其中 0，1 称为格$(L,\leqslant)$的界。

据定义，显然有限格一定是有界格，因为，

$$a_1 \times \cdots \times a_n = 0$$

$$a_1 \oplus \cdots\cdots \oplus a_n = 1$$

引理 2　若$(L,\times,\oplus,0,1)$是有界格，则对任意 $a\in L$，恒有

$$a \oplus 0 = a, a \times 1 = a, a \oplus 1 = 1, a \times 0 = 0$$

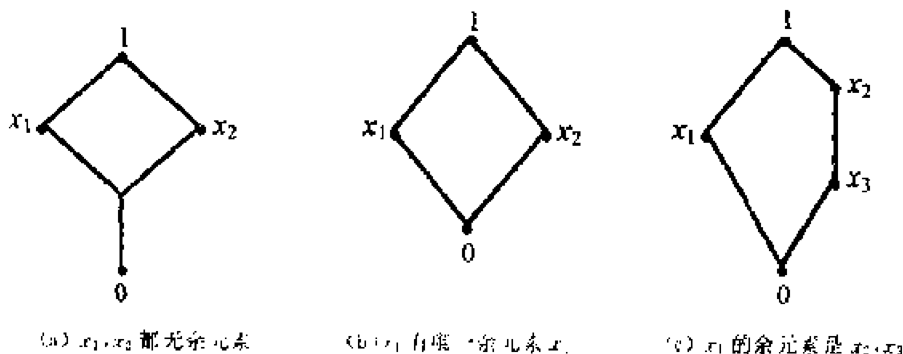
证明留给读者。

定义　在有界格$(L,\times,\oplus,0,1)$中，一个元素 $b\in L$，称为元素 $a\in L$ 的*余元素*，如果

$$a \times b = 0, a \oplus b = 1。$$

据定义，在有界格$(L,\times,\oplus,0,1)$中，任意元素 a 可以有余元素，也可以没有余元素；如果有余元素，则可以有一个或一个以上的余元素。

例如，如图 8.4.1 的 Hasse 图所示的有界格，就说明了上述这些情况的存在。



(a) x_1,x_2 都无余元素　(b) x_1 有唯一余元素 x_2　(c) x_1 的余元素是 x_2,x_3

图 8.4.1

引理 3　在有界格$(L,\times,\oplus,0,1)$中，1 是 0 的唯一一个余元素，反之亦然。

证明：由引理 2 知

$$0 \times 1 = 0, 0 \oplus 1 = 1,$$

所以，0，1 互为余元素。

唯一性：若 $c\in L$，且 $c\neq 1$，c 是 0 的余元素，则

$$0 \times c = 0, 0 \oplus c = 1$$

又由引理 2 知，

$$0 \oplus c = c。$$

所以，$c=1$，矛盾。

同理可证 0 是 1 的唯一一个余元素

定义 有界格$(L,\times,\oplus,0,1)$说是一个有余格，如果对 L 中每一个元素，都至少有一个余元素。

例如，n 维格$(L^n,\leqslant_n)$是一个有余格，其中 $1_n=(1,\cdots,1)$，$0_n=(0,\cdots,0)$是界，$(a_1,\cdots,a_n)$的余元素为$(b_1,\cdots,b_n)$，其中

$$b_i = 0 \Leftrightarrow a_i = 1$$

$$b_i = 1 \Leftrightarrow a_i = 0$$

$$i = 1,\cdots,n$$

定义 格$(L,\times,\oplus)$称为分配格，如果对任意 $a,b,c\in L$，恒有

$$a \times (b \oplus c) = (a \times b) \oplus (a \times c)$$

$$a \oplus (b \times c) = (a \oplus b) \times (a \oplus c)$$

指出一点，分配格定义中的两个等式是等价的。亦即，在格中，只要有一个分配恒等式成立，另一个分配恒等式可以由格的性质推导出来，这一点作为习题留给读者。

不是所有的格都是分配格，例如，图 8.4.2 的 Hasse 图表示的两个格不是分配格：

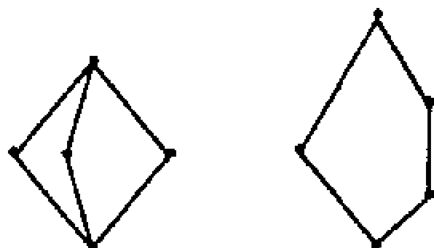


图 8.4.2

引理 4 任意一个链都是一个分配格。

证明：设格$(L,\leqslant)$是一个链，对 $a,b,c\in L$ 有下面两种情况。

(1) $a\geqslant b, a\geqslant c$，于是：$a\geqslant b\oplus c$，故

$$a \times (b \oplus c) = b \oplus c$$

而 $a\times b=b, a\times c=c$，所以

$$(a \times b) \oplus (a \times c) = b \oplus c$$

故 $a\times(b\oplus c)=(a\times b)\oplus(a\times c)$。

(2) $a\leqslant b$ 或者 $a\leqslant c$，不妨设 $a\leqslant b$，于是

$$a \leqslant (b \oplus c)$$

故 $a\times(b\oplus c)=a$ 而

$$(a \times b) \oplus (a \times c) = a \oplus (a \times c) = a$$

故 $a\times(b\oplus c)=(a\times b)\oplus(a\times c)$。

例如，自然数关于整除所得的格是分配格。

可以验证$[a,(b,c)]=([a,b],[a,c])$

又如，幂集合是分配格，因交对并有分配律；同理 n 维格也是分配格，因与幂集合格同构。再如，子群格不是分配格，如 Klein 四元群的子群格。

定理 1　(De Morgan 定律) 设$(L,\times,\oplus)$是一个分配格，对任意元素 a,b，若 a,b 有余元素 a',b'，则

$$(a \times b)' = a' \oplus b'$$
$$(a \oplus b)' = a' \times b'$$

证明：因为

$$\begin{aligned}&(a' \ominus b') \ominus (a \times b)\\ &= (a' \oplus b' \oplus a) \times (a' \ominus b' \ominus b)\\ &= (1 \oplus b') \times (a' \oplus 1) = 1 \times 1 = 1\end{aligned}$$

而

$$\begin{aligned}&(a' \ominus b') \times (a \times b)\\ &= (a' \times a \times b) \oplus (b' \times a \times b)\\ &= (0 \times b) \oplus (0 \times a)\\ &= 0 \oplus 0 = 0\end{aligned}$$

由余元素定义知，

$$(a \times b)' = a' \oplus b'$$

同理可证另一等式。

定义　设$(L,\leqslant)$是一个格，对任意 $a,b,c \in L$，如果 $a \leqslant b$，都有

$$a \oplus (b \times c) = b \times (a \oplus c)$$

则称$(L,\leqslant)$为模格。

显然，任意分配格是模格。

例如，群 G 中的所有正规子群作成的格是模格。

(1)设 G 是群，A,B 是其正规子群，定义 $AB=\{xy \mid (x \in A) \wedge (y \in B)\}$，则 AB 也是 G 的正规子群。(事实上是 A,B 生成的子群)。

证明：首先，AB 是子群(第六章§3，习题 6)。

往证对任 $g \in G$，$gABg^{-1} \subseteq AB$，对任 $g \in G$，任取 $\mu \in g(AB)$，设 $\mu = gab$，其中 $a \in A$，$b \in B$，因为 A,B 是正规子群，所以，$gab = a_1gb = a_1b_1g$，其中 $a_1 \in A$，$b_1 \in B$，故 $\mu = gab \in (AB)g$，所以 $g(AB) \subseteq (AB)g$，$gABg^{-1} \subseteq AB$，即 AB 是正规子群。

(2)设群 G 的所有正规子群的集合为 S，乘运算规定为交运算$\cap$，加运算规定为(1)中定义的乘运算，则$(S,\cap,\cdot)$是格。

证明：首先满足结合律，显然。

其次，交运算$\cap$满足交换律，显然。

看乘运算，需证 $AB=BA$。

任取 $\mu \in AB$，$\mu = ab$，其中 $a \in A$，$b \in B$，因为 B 是正规子群，所以 $ab = b_1a(b_1 \in B)$，所以 $\mu \in BA$，即 $AB \subseteq BA$。

同理 $BA \subseteq AB$，所以 $AB=BA$。

最后证满足吸收律，即要证 $A(A \cap B)=A$，$A \cap (AB)=A$。

证前一个，任取 $\mu \in A(A \cap B)$，则 $\mu = ac$，$a \in A$，$c \in A \cap B \subseteq A$，所以 $c \in A$，即 $\mu \in A$，所以 A

$(A\cap B)\subseteq A$。

任取 $\mu\in A$，因为 $1\in A\cap B$，所以 $\mu=\mu 1\in A(A\cap B)$，所以 $A\subseteq A(A\cap B)$

即 $A(A\cap B)=A$，另一式可类似证明。

(3) 证$(S,\cap,\cdot)$是模格。

往证，若 $a\leqslant b$，则 $a\oplus(b\times c)=b\times(a\oplus c)$

需明确与此代数格等价的半序关系。因交运算是集合交，故等价的半序关系是群子集的包含于关系。

所以需证，对 $A,B,C\in S$，若 $A\subseteq B$，则 $A(B\cap C)=B\cap(AC)$

任取 $\mu\in A(B\cap C)$，于是 $\mu=ad$，其中 $a\in A$，$d\in B\cap C$，当然 $d\in B$，$d\in C$，所以 $\mu\in AC$，又因为 $a\in A\subseteq B$，$d\in B$ 所以，$\mu\in B$，所以，$\mu\in B\cap(AC)$，即 $A(C\cap B)\subseteq(AC)\cap B$

另一方面，任取 $\mu\in(AC)\cap B$，则 $\mu\in AC$ 并且 $\mu\in B$，令 $\mu=ad$，其中 $a\in A$，$d\in C$，则 $d=a^{-1}\mu$，因为 $a^{-1}\in A\subseteq B$，而 $\mu\in B$，所以 $a^{-1}\mu\in B$，即 $d\in B$，故 $d\in B\cap C$，即 $\mu=ad\in A(B\cap C)$，即$(AC)\cap B\subseteq A(C\cap B)$。

综上，$A(B\cap C)=B\cap(AC)$，所以是模格。

定理 2 格$(L,\leqslant)$是模格的充分必要条件是：对任意 $a,b,c\in L$，如果 $a\leqslant b$，$a\times c=b\times c$，$a\oplus c=b\oplus c$，则必有 $a=b$。

证明：⇒)若格$(L,\leqslant)$是模格，如果 $a\leqslant b$，$a\times c=b\times c$，$a\oplus c=b\oplus c$，则

$$
\begin{aligned}
a&=a\oplus(a\times c)\\
&=a\oplus(b\times c)\\
&=b\times(a\oplus c)\\
&=b\times(b\oplus c)\\
&=b
\end{aligned}
$$

⇐)要证是模格，应证满足若 $a\leqslant b$，则有 $a\oplus(b\times c)=b\times(a\oplus c)$
由上节定理 4，可知因为 $a\leqslant b$，则 $a\oplus(b\times c)\leqslant b\times(a\oplus c)$。

设 $x=a\oplus(b\times c)$，$y=b\times(a\oplus c)$

已有 $x\leqslant y$，需证 $x=y$，由已知可知，只须证 $x\times c=y\times c$，$x\oplus c=y\oplus c$

因为，$x\oplus c=(a\oplus(b\times c))\oplus c=a\oplus((b\times c)\oplus c)=a\oplus c$，而由 $a\leqslant b$ 知，$a\leqslant b\times(a\oplus c)=y$，即 $a\oplus c\leqslant y\oplus c\leqslant(a\oplus c)\oplus c=a\oplus c$，故 $y\oplus c=a\oplus c$，所以 $x\oplus c=y\oplus c$。即若 $a\leqslant b$，则 $x\oplus c=y\oplus c$。同理可证：当 $a\leqslant b$ 时，有$(b\times(a\oplus c))\times c=(a\oplus(b\times c))\times c$，所以有 $y\times c=x\times c$，所以 $x=y$。

定理 3 设格$(L,\times,\oplus)$是分配格，对任意 $a,b,c\in L$，如果 $a\times b=b\times a$，$a\oplus c=b\oplus c$，则有 $a=b$。

证明：若$(L,\times,\oplus)$是分配格，且 $a\times c=b\times c$，$a\oplus c=b\oplus c$，则

$$
\begin{aligned}
a&=a\times(a\oplus c)=a\times(b\oplus c)\\
&=(a\times b)\oplus(a\times c)\\
&=(a\times b)\oplus(b\times c)\\
&=b\times(a\oplus b)\\
&=b\times(b\oplus c)=b
\end{aligned}
$$

说明在分配格中消去律成立。

推论 设格$(L,\times,\oplus)$是一个有余分配格，则对任意 $a\in L$，a 的余元素 a' 是唯一的。

证明：因$(L,\times,\oplus)$是一个有余格，设 a' 和 a'' 都是 a 的余元素，则

$$a \times a' = 0, a \oplus a' = 1$$
$$a \times a'' = 0, a \oplus a'' = 1$$
$$a \times a' = a \times a'', a \oplus a' = a \oplus a'',$$

由定理 3，$a'=a''$。

习　　题

1. 证明：在有余分配格$(L,\times,\oplus)$中，对任意 $a,b\in L$，有
$$a \leqslant b \Leftrightarrow a \times b' = 0$$
$$b' \leqslant a' \Leftrightarrow a' \oplus b = 1$$
$$a \leqslant b \Leftrightarrow b' \leqslant a'$$
2. 证明：在格$(L,\times,\oplus)$中，若第一分配律成立，则第二分配律成立，反之亦然。
3. 证明：§4 中的引理 1，引理 2。

§5　布尔代数

定义　一个有余分配格称为一个布尔代数。

因为布尔代数是一个格，今后将布尔代数中的运算$\times$简记为.，称为乘法。运算$\oplus$简记为+，称为加法。因为布尔代数是有界格，将最大元记为 1，最小元记为 0。因为布尔代数是有余分配格，所以，对布尔代数中任意元素 a，有唯一的余元素 a'，因此，这是布尔代数上的一个一元运算，称为余运算，记为$-$。

所以，布尔代数 B，可记为$(B,\cdot,+,-,0,1)$。今后，有时将 $a.b$ 简记为 ab。

下面我们给出布尔代数的一些重要性质，但这些性质之间并不是互相独立的。

(一) $(B,\cdot,+)$是一个格，所以有

1) $aa=a$　　1') $a+a=a$

2) $ab=ba$　　2') $a+b=b+a$

3) $(ab)c=a(bc)$　　3') $(a+b)+c=a+(b+c)$

4) $a(a+b)=a$　　4') $a+(ab)=a$

(二) $(B,\cdot,+)$是分配格，所以有

5) $a(b+c)=(ab)+(ac)$　　5') $a+(bc)=(a+b)(a+c)$

6) $(ab)+(ac)+(bc)=(a+b)(a+c)(b+c)$

7) 若 $ab=ac, a+b=a+c$，则 $b=c$

(三) 因$(B,\cdot,+,0,1)$是有界格，所以有

8) $0\leqslant a\leqslant 1$

9) $a0=0$　　9') $a+1=1$

10) $a1=a$　　10') $a+0=a$

(四) 因$(B,\cdot,+,-,0,1)$是有余分配格，所以有

11) $a\bar{a}=0$　　11') $a+\bar{a}=1$

12) $\bar{0}=1$　　12') $\bar{1}=0$

13) $(\overline{ab}=\bar{a}+\bar{b})$　　13') $(\overline{a+b})=\bar{a}\bar{b}$

（五）$(B,\leqslant)$是半序格，所以有

14）$ab=\inf\{a,b\}$　　14'）$a+b=\sup\{a,b\}$

15）$a\leqslant b\Leftrightarrow a+b=b\Leftrightarrow ab=a$

16）$a\leqslant b\Leftrightarrow a\bar{b}=0\Leftrightarrow \bar{b}\leqslant\bar{a}\Leftrightarrow \bar{a}+b=1$

有上述性质的代数系统必是布尔代数，一个布尔代数，必有上述性质，但上述性质不是互相独立的，下面我们用互相独立的 Huntington 公理来定义布尔代数。

定理1　设 B 是一个至少含有两个不同元素的集合，$\cdot$，$+$是定义在 B 上的两种代数运算，如果对任意 $a,b,c\in B$，满足下面公理：

H_1：$ab=ba$，$a+b=b+a$

H_2：$a(b+c)=(ab)+(ac)$

$a+(bc)=(a+b)(a+c)$

H_3：B 中有元素 0 和元素 1，使得对任意 $a\in B$，有

$$a1=a,a+0=a$$

H_4：对任意 $a\in B$，有 $\bar{a}\in B$，使得

$$a\bar{a}=0\qquad a+\bar{a}=1$$

则$(B,\cdot,+,-,0,1)$是一个布尔代数。

证明：只须证明$(B,\cdot,+)$是格，并且 0，1 是最小最大元素，再由 H_4 为有余格，由 H_2 为分配格。

要证是格，须证有交换律，结合律，吸收律，我们分别只证一个等式。

(1) 交换律：由 H_1 知成立。

(2) 吸收律：因为 $1+b=(1+b)1=(1+b)(b+\bar{b})=b+\bar{b}1=1$

所以 $a+(ab)=a1+ab=a(1+b)=a1=a$。

(3) 结合律：先证在假设 $H_1\sim H_4$ 条件下，若 $a+b=a+c$，$\bar{a}+b=\bar{a}+c$，则 $b=c$。

由$(a+b)(\bar{a}+b)=b+a\bar{a}=b+0=b$

$(a+b)(\bar{a}+b)=(a+c)(\bar{a}+c)=c+a\bar{a}=c+0=c$

所以 $b=c$。

设 $L=a(bc)$，$M=(ab)c$

须证 $a+L=a+M$，$\bar{a}+L=\bar{a}+M$ 即可。

$a+L=a+(a(bc))=a$

$a+M=a+((ab)c)=(a+ab)(a+c)=a(a+c)=a$

所以 $a+L=a+M$

$\bar{a}+L=\bar{a}+(a(bc))=1(\bar{a}+bc)=1(\bar{a}+b)(\bar{a}+c)$

$\bar{a}+M=\bar{a}+((ab)c)=(\bar{a}+ab)(\bar{a}+c)=1(\bar{a}+b)(\bar{a}+c)$

所以 $\bar{a}+L=\bar{a}+M$，

即 $M=L$，故结合律成立。

最后证有界性。为此需明确半序关系，自然应规定：

$$a\leqslant b\Leftrightarrow ab=a\Leftrightarrow a+b=b.$$

由 H_3 知，

$$a1=a，得 a\leqslant 1$$

$$a+0=a，得 0\leqslant a$$

所以 $0\leqslant a\leqslant 1$。故 0,1 是最小最大元素。因此$(B,\cdot,+,-,0,1)$是布尔代数。

还可证明:$H_1\sim H_4$ 是独立的。公理体系是独立的,指其中任一公理不能由其余的公理推导出来,证明某公理体系中公理独立,如公理 A 独立,可给出一个模型,它不满足 A 而满足其余所有公理,这个模型的存在就证明了公理 A 是独立的。我们省略这个证明。有兴趣的读者可参看 R. L. Goodstein 所著"Boolean Algebra"。

例如(电路代数),设 $B=\{0,1\}$,B 上的运算一,.,+,如下表定义:

.	0	1
0	0	0
1	0	1

+	0	1
0	0	1
1	1	1

x	$\bar{x}$
0	1
1	0

不难证明:$(B,\cdot,+,-,0,1)$是布尔代数。这是最简单的一个布尔代数。

又如,集合代数$(\rho(A),\cap,\cup,\sim,\phi,A)$是一个布尔代数;命题代数$(S,\wedge,\vee,\neg,F,T)$

再如(开关代数),设 B_n 是由 0,1 做分量的所有 n 元向量集合。对任意 $a,b\in B_n$,令

$$a=(a_1,\cdots,a_n),b=(b_1,\cdots,b_n),$$

定义 B_n 上的运算如下:

$$ab=(a_1b_1,a_2b_2,\cdots,a_nb_n)$$
$$a+b=(a_1+b_1,a_2+b_2,\cdots,a_n+b_n)$$
$$\bar{a}=(\bar{a}_1,\bar{a}_2,\cdots,\bar{a}_n)$$

不难证明:$(B_n,\cdot,+,-,0_n,1_n)$是一个布尔代数,其中 0_n 表示 n 个 0 做成的 n 元向量,1_n 表示 n 个 1 做成的 n 元向量。

下面,如不特别指出,我们在本节提到的布尔代数都是有限布尔代数。

定义　任给一个布尔代数$(B,\cdot,+,-,0,1)$。若 B 的一个子集 S 包含 0,1,且$(S,\cdot,+,-,0,1)$仍是一个布尔代数,则称 S 为 B 的子代数。

例如,$A=\{a,b,c\}$,$(\rho(A),\cap,\cup,\sim,\phi,A)$是集合代数,

其中 $B=\{\phi,\{c\},\{a,b\},\{a,b,c\}\}$是一个子代数;

$C=\{\phi,\{a\},\{c\},\{a,c\}\}$则不是一个子代数。

C 看做代数格时,是代数子格,这四个元素也可以做成布尔代数,最大元是$\{a,b\}$,但它不是原布尔代数的子代数。

又如,设$(B,\cdot,+,-,0,1)$是任意布尔代数,则$\{0,1\}$是子代数。

定理 2　设$(B,\cdot,+,-,0,1)$是布尔代数,于是,B 的子集 S 是 B 的子代数的充要条件是 S 在运算.,+,-下是封闭的。

证明:必要性显然。

充分性,若 S 在.,+,-下封闭,对 $a\in S$,则 $\bar{a}\in S$,所以 $a+\bar{a}=1\in S$,$a\bar{a}=0\in S$。故 S 中有 0,1,又因为 $S\subseteq B$,S 中元做为 B 中元也适合 $H_1\sim H_4$,所以 S 是子代数。

定义　设$(B,\cdot,+,-,0,1)$是布尔代数,$e_1,\cdots,e_n$ 是 B 中有如下性质的一组元素:

对任意 $a\in B$,都可唯一地表示为

$$a=\alpha_1e_1+\alpha_2e_2+\cdots+\alpha_ne_n$$

其中 α_i 或为 0,或为 1,$(i=1,\cdots,n)$,则称 $e_1,\cdots,e_n$ 为布尔代数 B 的一组基底,并称此布尔代数为 n 维的。

显然，基底中无0，因若不然，有0.0的系数可任意而表法不唯一。

例如，$S=\{a,b,c\}$，看布尔代数$(\rho(S),\cap,\cup,\sim,\phi,S)$，则$\{a\}$，$\{b\}$，$\{c\}$是基底。

请读者自己证明。

定义 设$(B,\cdot,+,-,0,1)$是布尔代数。若B中非零元素a有性质：对任意$x\in B$，ax或者为0，或者为a，则称a为布尔代数B的极小元素。

直观地看，极小元素在Hasse图中恰是直接在0上面的那一层。

显然，布尔代数中两个不同极小元素a,b，必有$ab=0$。

引理1 设B是布尔代数，a是B中任一非零元素，若a不是极小元素，则存在极小元素b，使$b<a$。

证明：因为a不是极小元素，则必有某非零元素x_0，使得$ax_0\neq 0$，且$ax_0\neq a$。

令$ax_0=a_1$，则$a_1<a$。

若a_1仍不是极小元素，则有非零元素x_1，使$a_1x_1\neq 0$，且$a_1x_1\neq a_1$，

令$a_1x_1=a_2$，显然，$a_2<a_1$。

重复上述过程，由于B中元素有限，必存在极小元素$a_n=b$，使得

$$a_n<a_{n-1}<\cdots<a$$

所以$b<a$。

在Hasse图中直观地看，任非零元素下行必通过某个极小元素到达0。

定理3 有限布尔代数的基底必是此代数的所有极小元素。反之，此代数的所有极小元素必然做成此代数的基底。

1）要证(1) 基底中元是极小元素。

(2) 极小元素必在基底中。

证明：(1)设$e_1,\cdots,e_n$是B的基底，往证e_i是极小元素。

若不然，则必有$a\in B$，使$ae_i=b$，而$b\neq 0$且$b\neq e_i$，以下推出$b=0$或$b=e_i$而矛盾。

显然，$b\leq e_i$，故$be_i=b$。

令$b=\alpha_1e_1+\cdots+\alpha_ne_n$，再取$c=\bar{b}e_i$，则$b+c=be_i+\bar{b}e_i=e_i$，令

$$c=\beta_1e_1+\cdots+\beta_ne_n$$

于是有

$$e_i=b+c=(\alpha_1+\beta_1)e_1+\cdots+(\alpha_n+\beta_n)e_n$$

由基底的性质，必有

$$\alpha_j=\beta_j=0,(j\neq i,j=1,\cdots,n),$$
$$\alpha_i+\beta_i=1,\alpha_i=1\text{ 或 }\beta_i=1.$$

若$\alpha_i=1$，则$b=e_i$，矛盾。

若$\beta_i=1$，则$c=e_i$，即$\bar{b}e_i=e_i$，所以$b=be_i=b(\bar{b}e_i)=(b\bar{b})e_i=0e_i=0$，矛盾。

综上，e_i是极小元素。

(2) 设e^*是极小元素。令

$$e^*=\alpha_1e_1+\cdots+\alpha_ne_n$$

因为$e^*\neq 0$，故不妨设$\alpha_j\neq 0$，这样，$\alpha_j=1$，因已证$e_1,\cdots,e_n$是极小元素，所以$e_ie_j=0$，当$i\neq j$时，于是

$$e^*e_j=\alpha_1e_1e_j+\cdots+\alpha_ne_ne_j=1e_j=e_j$$

再由 e^* 是极小元素，$e^* e_j \neq 0$，所以 $e^* e_j = e^*$ 即 $e^* = e_j$，所以 e^* 是基底中某一元素。

2) 证所有极小元素做成基底。

证明：(事实上，任一元素正好唯一表为小于等于它的极小元素和)。设 $e_1,\cdots,e_n$ 是所有极小元素。

首先，$e_i = 0e_1 + \cdots + 1e_i + \cdots + 0e_n$

此表示唯一，因若不然，$e_i = \alpha_1 e_1 + \cdots + \alpha_n e_n$，其中必至少有一个 $\alpha_j \neq 0 (j \neq i)$，于是

$$0 = e_i e_j = \alpha_1 e_1 e_j + \cdots + \alpha_n e_n e_j = \alpha_j e_j e_j = e_j，矛盾于 e_j \neq 0。$$

其次，设 a 是 B 中任一非极小元素，由引理 1 小于它的极小元存在，设全体为

$$e_{i1},\cdots,e_{ik},(1 \le i1 < \cdots < ik \le n),$$

令 $b = e_{i1} + \cdots + e_{ik}$，显然 $b \le a$。

若 $b<a$，则 $\bar{b}a \neq 0$(否则，将推出 $a \le b$)。于是由引理 1 有极小元素 $e_j \le \bar{b}a$。因为 $\bar{b}a \le a$，所以 $e_j \le a$，因此 e_j 是 $e_{i1},\cdots,e_{ik}$ 中一个。

设 $e_j = e_{il} (1\le l \le k)$。因为 $e_j = e_{il} \le \bar{b}a$，所以 $(\bar{b}a)e_{il} = e_{il}$ 而 $e_{il}b = e_{il}$(因为 $e_{i1}+\cdots+e_{il}+\cdots+e_{ik} = b$ 两边乘 e_{il} 即得)，故 $(\bar{b}a)e_{il}b = e_{il}$，即 $e_{il} = (b\bar{b})ae_{il} = 0$，矛盾，故 $b=a$，即 $a = e_{i1}+\cdots+e_{ik}$ 得证。

再证表示唯一。

设又有 $a = e_{j1}+\cdots+e_{jr}$ 是不同表示。不妨设 e_{j1} 不在 $e_{i1},\cdots,e_{ik}$ 中出现。于是在 $a = e_{j1}+\cdots+e_{jr}$ 两边用 e_{j1} 乘，得 $e_{j1}a = e_{j1}$；在 $a = e_{i1}+\cdots+e_{ik}$ 两边用 e_{j1} 乘，得 $e_{j1}a = 0$，这样 $e_{j1}=0$ 矛盾，证毕。

推论 1　若 $(B,\cdot,+,-,0,1)$ 是布尔代数，其基底为 $e_1,\cdots,e_n$，则 $e_1+e_2+\cdots+e_n = 1$。

推论 2　有限布尔代数的基底是唯一的。

定义　设 $(B,\cdot,+,-,0,1)$ 是布尔代数，$s_1,\cdots,s_r$ 是 B 中一组元素，设 S 是关于 $s_1,\cdots,s_r$ 的所有多项式的集合：

$$\sum x_{i1}\cdots x_{in}$$

其中 $1\le ip \le r$ $(1\le p\le n)$，x_{ip} 或为 s_{ip} 或为 $\overline{s_{ip}}$，不难证明：$(S,\cdot,+,-,0,1)$ 是布尔代数，我们称此布尔代数为由 $\{s_1,\cdots,s_r\}$ 生成的布尔代数。

定义　设 $X_1\cdots,X_n$ 是一组文字，于是文字串 $X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}$ 称为关于 $X_1,\cdots,X_n$ 的一个极小项，其中 αi 或为 0，或为 1，$i=1,\cdots,n$。

关于布尔代数 B 中一组元素 $s_1,\cdots,s_r$ 的极小项就是关于 $s_1,\cdots,s_r$ 的极小项，并规定

$$s_i^0 = \bar{s}_i, s_i^1 = s_i。$$

极小项性质：

(1) 关于 n 变元极小项共 2^n 个(因为看有 n 个位置，每位置可取 0 或 1)。

(2) 对每个极小项，恰有一个 B 中 0,1 组成的 n 元值组，代入该极小项后值为 1，不同极小项对应的那个 n 元值组不同，于是，每个极小项唯一对应一个二进制数，改为十进制是 p，此极小项记为 m_p，关于 $s_1,\cdots,s_n$ 的多项范式即为一些极小项的和。

定义　布尔代数 B 中一组元素 $A_1,\cdots,A_n$ 称为互相独立的，如果关于它们的所有极小项都不为 0。

定理 4　设 B 是布尔代数，$A_1,\cdots,A_n$ 是其中一组互相独立的元素，设 A 是由 $\{A_1,\cdots,A_n\}$ 生成的布尔代数，于是对于 A 中任意元素 a，都可唯一地表成一个关于 $A_1,\cdots,A_n$ 的多项范式。

证明：(先证能表成)对 A 中任意 a，由生成定义，a 可表为关于 $A_1,\cdots,A_n$ 的多项式，若其中某项 p 不是极小项，缺少的是 $A_{i1},\cdots,A_{ik}$，可乘 $(A_{i1}+\overline{A_{i1}})\cdots(A_{ik}+\overline{A_{ik}})$，再用分配律展开即

化 p 为极小项和。

（再证唯一性）若不然，G,H 是 a 的两种不同的多项范式，则至少有某极小项 m_i 或在 G 不在 H 中，或在 H 不在 G 中，不妨假定是前者，注意不同的极小项相乘为零，这时在 $a=G$ 两边乘 m_i 得，$am_i=(G)m_i=m_i$，在 $a=H$ 两边乘 m_i 得 $am_i=(H)m_i=0$，这样 $m_i=0$ 矛盾。

推论 设 B 是布尔代数，A 是由互相独立元素 $\{A_1,\cdots,A_n\}$ 生成的布尔代数，于是关于 $A_1,\cdots,A_n$ 的 2^n 个极小项 $m_0,\cdots,m_{2^n-1}$ 是布尔代数 A 的基底。

定理 5 设 A 是由互相独立的元素 $\{A_1,\cdots,A_n\}$ 生成的布尔代数，于是 A 中所有极小元素就是关于 $A_1,\cdots,A_n$ 的所有极小项。

证明：由定理 3，A 的基底是所有极小元素，由定理 4，及其推论得 A 的基底是所有极小项，基底是唯一确定的，故所有极小元素是所有极小项。

定义 设 $(B,\cdot,+,\bar{\ },0,1)$ 和 $(S,\wedge,\vee,\neg,\alpha,\beta)$ 是两个布尔代数，B 到 S 的映射 f，称为两个布尔代数间的同态映射，如果对任意 $a,b\in B$，有

$$f(ab)=f(a)\wedge f(b)$$
$$f(a+b)=f(a)\vee f(b)$$
$$f(\bar{a})=\neg f(a)$$
$$f(0)=\alpha$$
$$f(1)=\beta$$

显然，$f(B)$ 是 S 的子代数，称布尔代数 $f(B)$ 是布尔代数 B 的同态象，如果 B 到 S 上的同态映射 f 是一对一映射，则称 f 为同构映射，也称 B 与 S 同构。

引理 2 设 f 是布尔代数 $(B,\cdot,+,-,0,1)$ 到布尔代数 $(S,\wedge,\vee,\neg,\alpha,\beta)$ 的一个映射。如果对任意 $a,b\in B$，都有

$$f(ab)=f(a)\wedge f(b)$$
$$f(\bar{a})=\neg f(a)$$

则 f 是 B 到 S 的同态映射。

引理 3 设 f 是布尔代数 $(B,\cdot,+,-,0,1)$ 到布尔代数 $(S,\wedge,\vee,\neg,\alpha,\beta)$ 的一个映射。如果对任意 $a,b\in B$，都有

$$f(ab)=f(a)\wedge f(b)$$
$$f(a+b)=f(a)\vee f(b)$$

则 $(f(B),\wedge,\vee,\neg,f(0),f(1))$ 是一个布尔代数，且 f 是 B 到 $f(B)$ 的同态映射。其中 $\neg$ 是关于 $f(0)$、$f(1)$ 的余运算。

引理 4 设 $(B,\cdot,+,-,0,1)$ 和 $(S,\wedge,\vee,\neg,\alpha,\beta)$ 是两个布尔代数。f 是 B 到 S 上的映射。如果对任意 $a,b\in B$，都有

$$f(ab)=f(a)\wedge f(b)$$
$$f(a+b)=f(a)\vee f(b)$$

则 f 是 B 到 S 上的同态映射。

定理 6 如果两个有限布尔代数的维数相同，则这两个代数同构。

证明：设布尔代数 $(B,\cdot,+,-,0,1)$ 和 $(S,\wedge,\vee,\neg,\alpha,\beta)$ 都是 n 维的，其基底分别为 $e_1,\cdots,e_n$ 和 $u_1,\cdots,u_n$。

作 B 到 S 的映射 f 如下：

$$e_i \xrightarrow{f} u_i \quad i=1,\cdots,n$$

$$\sum_{i=1}^{n}{}^{(1)}\alpha_i e_i \xrightarrow{f} \sum_{i=1}^{n}{}^{(2)}\alpha_i^f \wedge u_i$$

其中：$\sum_{i=1}^{n}{}^{(1)}a_i$ 是 $a_1+\cdots+a_n$ 的缩写；$\sum_{i=1}^{n}{}^{(2)}b_i$ 是 $b_1 \vee \cdots \vee b_n$ 的缩写；

$$\alpha_i = 0 \text{ 或 } 1;$$

$$\alpha_i^f = \begin{cases} \alpha, & \alpha_i = 0 \\ \rho, & \alpha_i = 1 \end{cases} \quad i=1,\cdots,n$$

则不难验证 f 是一对一映射且 $f(B)=S$。

下面证明同态性．设

$$a = \sum_{i=1}^{n}{}^{(1)}\alpha_i e_i$$

$$b = \sum_{i=1}^{n}{}^{(1)}\beta_i e_i$$

于是

$$f(a) = \sum_{i=1}^{n}{}^{(2)}\alpha_i^f \wedge u_i$$

$$f(b) = \sum_{i=1}^{n}{}^{(2)}\beta_i^f \wedge u_i$$

所以

$$\begin{aligned} f(a+b) &= f\left(\sum_{i=1}^{n}{}^{(1)}(\alpha_i+\beta_i)e_i\right) \\ &= \sum_{i=1}^{n}{}^{(2)}((\alpha_i+\beta_i)^f \wedge u_i) \\ &= \sum_{i=1}^{n}{}^{(2)}((\alpha_i^f \vee \beta_i^f) \wedge u_i) \\ &= \left(\sum_{i=1}^{n}{}^{(2)}\alpha_i^f \wedge u_i\right) \vee \left(\sum_{i=1}^{n}{}^{(2)}\beta_i^f \wedge u_i\right) \\ &= f(a) \vee f(b) \end{aligned}$$

同理可证：

$$f(ab) = f(a) \wedge f(b)$$

由引理 4 知，B 与 S 同构。

定理 7　任意 n 维布尔代数 $(B,\cdot,+,-,0,1)$ 与开关代数 $(B_n,\cdot,+,-,0_n,1_n)$ 同构。

证明：因为 $(1,0,\cdots,0),(0,1,0,\cdots,0),\cdots,(0,\cdots,0,1)$ n 个向量是 B_n 的一组基底，故 B_n 是 n 维的，由定理 6 知，B 与 B_n 同构。

定理 8(Stone 定理)　任意有限布尔代数 $(B,\cdot,+,-,0,1)$ 与某个集合 S 的幂集合做成的布尔代数 $(\rho(S),\cap,\cup,\sim,\phi,S)$ 同构。

证明：设布尔代数 B 的基底为 $e_1,\cdots,e_n$，令集合 $S=\{e_1,\cdots,e_n\}$，显然，布尔代数 $(\rho(S),\cap,\cup,\sim,\phi,S)$ 的基底为 $\{e_1\},\{e_2\},\cdots,\{e_n\}$，故 $\rho(S)$ 是 n 维的，由定理 6，B 与 $\rho(S)$ 同构。

习　　题

1. 设$(B,\cdot,+,\bar{\ },0,1)$是布尔代数,定义 B 上两种代数运算如下:

$$a \oplus b = (a\bar{a}) - (\bar{a}b)$$

$$a \times b = ab$$

于是,称代数$(B,\times,\oplus)$为布尔环。证明:在布尔环中,有如下性质:

1) $a\oplus a=0$

2) $a\oplus 0=a$

3) $a\oplus 1=\bar{a}$

4) $a\times(b\oplus c)=(a\times b)\oplus(a\times c)$

5) $a=b\Leftrightarrow a\oplus b=0$

6) $a\oplus b=\bar{a}\oplus\bar{b}$

7) $\overline{a\oplus b}=\bar{a}\oplus b=a\oplus\bar{b}$

8) 若 $a\times b=0$,则 $a\oplus b=a+b$

9) 若 $a\oplus c=b\oplus c$,则 $a=b$

2. 证明:§5 中引理 2,3,4

3. 设$(B,\cdot,+,-,0,1)$是$(2n+1)$维布尔代数,n 为任意自然数$(n\neq 0)$,若 B 中元素 a_1、$\cdots$、a_m 是 B 的生成元素,则 $a_1,\cdots,a_m$ 互相不独立。

4. 设$(B,\cdot,+,-,0,1)$是 n 维布尔代数,基底为 $e_1,\cdots,e_n$,S 是 B 的 m 维子代数$(m\leqslant n)$。证明:S 的基底必是如下 m 个元素:将 $e_1,\cdots,e_n$ 重新做某种排列,然后分割成 m 段,每段元素相加所得之 m 个元素。

5. 在布尔代数中,证明下列等式:

1) $a+(\bar{a}b)=a+b$

2) $a(\bar{a}+b)=ab$

3) $(ab)+(a\bar{b})=a$

4) $(a+b)(a+\bar{b})=a$

参 考 文 献

[1] 耿素云等编,《离散数学》,清华大学出版社,1992年。
[2] 刘光奇等编,《离散数学》,复旦大学出版社,1988年。
[3] 左孝凌等编,《离散数学》,上海科学技术出版社。
[4] 王朝瑞编,《图论》,人民教育出版社,1981年。
[5] 迟志敏等编,《近世代数》,吉林教育出版社,1987年。